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*

LE TEMPS EST VENU DE MODERNISER LES OUTILS DU 20e SIÈCLE

Commissariat
à la protection de
la vie privée du Canada

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*
Le temps est venu de moderniser les outils du 20e siècle

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

(819) 994-5444, 1-800-282-1376

Cat. No. IP51-1F-PDF

1913-3375

Suivez-nous sur Twitter : @PriveePrivacy

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

Septembre 2016

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

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*, pour la période allant du 1er janvier 2015 au 31 mars 2016, et la *Loi sur la protection des renseignements personnels*, pour la période allant du 1er avril 2015 au 31 mars 2016.

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

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

Original signé par

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

Septembre 2016

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

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*, pour la période allant du 1er janvier 2015 au 31 mars 2016, et la *Loi sur la protection des renseignements personnels*, pour la période allant du 1er avril 2015 au 31 mars 2016.

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

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

Original signé par

Daniel Therrien

Table des matières

Message du commissaire

La protection de la vie privée en 2016 : le temps est venu de moderniser les outils du 20e siècle

J'ai le plaisir de présenter au Parlement le rapport annuel 2015-2016 du Commissariat à la protection de la vie privée du Canada. À partir de cette année, nous présenterons un seul rapport concernant à la fois la *Loi sur la protection des renseignements personnels*, qui s'applique au secteur public fédéral, et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui s'applique aux organisations du secteur privé. En juin 2015, la LPRPDE a été modifiée de sorte que la période de rapport corresponde à celle prévue dans la *Loi sur la protection des renseignements personnels*. Ainsi, nous pouvons présenter un seul rapport annuel et non plus deux à des moments différents de l'année.

Internet n'existait pas au moment de la promulgation de la Loi sur la protection des renseignements personnels en 1983.

Le rythme constant et toujours plus rapide des changements technologiques et les répercussions profondes de ces changements sur la protection de la vie privée constituent un thème clé du présent rapport. Tant dans le secteur public que dans le secteur privé, une mise à jour des outils à notre disposition pour protéger les renseignements personnels des Canadiens s'impose. Autrement, nous risquons selon moi de miner la confiance des citoyens envers les institutions fédérales et l'économie numérique.

Grâce aux nouvelles technologies, les entreprises et les gouvernements peuvent recueillir et analyser des quantités infiniment plus grandes de renseignements en utilisant des algorithmes informatiques complexes. Cette capacité a donné lieu à des progrès dans divers domaines, depuis la mise au point de traitements sur mesure contre les maladies jusqu'à l'optimisation de la circulation routière.

Par ailleurs, les nouvelles technologies peuvent mener à des utilisations discutables des renseignements. Dans le secteur privé, des entreprises peuvent suivre à la trace les clients potentiels et analyser leur comportement comme jamais auparavant. Cette pratique ouvre la voie à des techniques de marketing envahissantes et aux services différenciés en fonction des caractéristiques présumées des gens. Dans le secteur public, les ministères et organismes fédéraux exerçant leurs activités dans le domaine de la sécurité nationale disposent désormais de pouvoirs accrus pour échanger des renseignements sur les interactions des Canadiens avec l'État. En analysant des mégadonnées, ils peuvent aussi dresser le profil de Canadiens ordinaires dans le but de repérer des menaces à la sécurité.

Il est très difficile de suivre le rythme de tous ces changements pour défendre et promouvoir le droit des individus à la vie privée comme le veut notre mission, d'autant plus que les lois sur la protection des

… **90 % des Canadiens** ont l'impression de perdre le contrôle qu'ils exercent sur leurs renseignements personnels et s'attendent à être mieux protégés.

renseignements personnels remontent à une époque où bon nombre de ces innovations technologiques n'avaient pas encore vu le jour. Internet n'existait pas au moment de la promulgation de la *Loi sur la protection des renseignements personnels* en 1983. Et Facebook n'avait pas encore germé dans l'esprit de ses concepteurs au moment de l'entrée en vigueur de la *Loi sur la protection des renseignements personnels et les documents électroniques* en 2001.

Nous disposons d'outils du 20e siècle pour résoudre des problèmes du 21e siècle. Entre-temps, 90 % des Canadiens ont l'impression de perdre le contrôle qu'ils exercent sur leurs renseignements personnels et s'attendent à être mieux protégés. Compte tenu de la rapidité et de l'ampleur des changements technologiques, il n'est pas étonnant que les Canadiens aient l'impression d'être mal renseignés sur les conséquences de ces changements sur leur droit à la vie privée et se sentent incapables d'exercer un contrôle sur leurs renseignements personnels. Dans cette situation, les organismes de réglementation, les législateurs, les tribunaux, les chefs d'entreprise et les autres décideurs doivent prendre des mesures plus énergiques pour protéger les citoyens.

C'est dans ce contexte que nous déposons le présent rapport annuel, qui porte sur les activités exercées par le Commissariat pour s'acquitter de sa mission au cours de la période visée, à savoir l'examen des plaintes; les avis au Parlement; les évaluations des facteurs relatifs à la vie privée et les vérifications; la sensibilisation du public; la réalisation et le financement de recherches sur les enjeux clés; la coopération internationale et fédérale-provinciale-territoriale; ainsi que les procédures judiciaires.

Le présent rapport fait état en détail de certains travaux importants que nous avons menés et que nous poursuivrons pour moderniser les cadres législatif, juridique et réglementaire du Canada afin de protéger la vie privée malgré les défis associés aux nouvelles technologies.

La réforme de la *Loi sur la protection des renseignements personnels*

L'évolution technologique constante a des répercussions considérables sur la vie privée. Il est très difficile de suivre le rythme de tous les changements, à plus forte raison sous le régime de lois qui ont été adoptées avant de nombreuses innovations technologiques ayant de telles répercussions.

Le chapitre 1 met en évidence les travaux que nous avons menés au cours du dernier exercice pour réformer la *Loi sur la protection des renseignements personnels*. Après plus de 30 ans, on observe un décalage entre cette loi et les risques d'atteinte à la vie privée actuels et à venir. En mars 2016, j'ai témoigné devant le Parlement. Je lui ai alors recommandé des modifications à cette loi axées sur trois grands thèmes :

- les changements technologiques;
- l'accroissement de la transparence;
- la modernisation des normes juridiques.

À l'époque de l'entrée en vigueur de la *Loi sur la protection des renseignements personnels*, l'information était recueillie et communiquée sur papier et les bureaux du gouvernement

fédéral étaient remplis de classeurs – des dizaines d'années avant l'avènement du courriel, des appareils mobiles et des médias sociaux. Aujourd'hui, il est possible de recueillir sans effort de vastes quantités de renseignements personnels et on peut encore plus facilement les perdre. Au cours des dernières années, des incidents de grande envergure portant sur des renseignements détenus par l'État ont touché des dizaines, voire des centaines de milliers de citoyens. Nous recommandons entre autres au Parlement d'obliger explicitement les institutions fédérales à protéger les renseignements personnels qui relèvent d'elles et à déclarer au Commissariat toute atteinte substantielle à la sécurité des données. Les entreprises privées sont déjà assujetties à ces obligations ou elles le seront bientôt.

De nos jours, les citoyens veulent à juste titre que les organisations leur expliquent de manière plus claire et détaillée l'utilisation qu'elles font de leurs renseignements personnels. Ils veulent de plus en plus savoir ce que les ministères font de leurs renseignements, à qui ils les communiquent et pour quelles raisons. Sous sa forme actuelle, la *Loi sur la protection des renseignements personnels* n'aide guère les Canadiens à trouver une réponse à ces questions. C'est d'ailleurs la raison pour laquelle nous avons recommandé de renforcer les obligations imposées aux institutions fédérales concernant les rapports de transparence et de limiter les exceptions s'appliquant aux demandes d'accès aux renseignements personnels en vertu de la Loi.

Entre autres recommandations, nous demandons aussi que la loi oblige les ministères à effectuer des évaluations des facteurs relatifs à la vie privée et à consulter le Commissariat avant de déposer des projets de loi susceptibles d'avoir des répercussions sur la vie privée. Le but est de faire en sorte que l'on puisse résoudre les problèmes en amont au lieu d'attendre que des personnes soient touchées. Nous recommandons aussi d'imposer une norme explicite selon laquelle seuls les renseignements personnels nécessaires à un programme ou à une activité gouvernementale pourraient être recueillis, de manière à éviter la collecte excessive que permettent les nouvelles technologies.

On trouvera dans le présent rapport de l'information plus détaillée sur les travaux menés par le Commissariat pour favoriser la modernisation de la loi sur la protection des renseignements personnels s'appliquant au secteur public fédéral.

Les priorités stratégiques liées à la vie privée

L'année dernière, le Commissariat a défini ses priorités après avoir mené de vastes consultations auprès des principaux intervenants et du public. Nous avons ainsi pu annoncer en mai 2015 les quatre priorités stratégiques liées à la protection de la vie privée qui orienteraient nos activités au cours des cinq années suivantes :

- l'économie des renseignements personnels;
- la surveillance du gouvernement;
- la réputation et la protection de la vie privée;
- le corps comme source d'information.

Le présent rapport fait des mises à jour importantes concernant nos travaux dans tous ces domaines clés et en émergence.

Le consentement et l'économie des renseignements personnels

En plus des changements nécessaires dans le secteur public, il est manifeste que nous devons également nous attaquer à des problèmes nouveaux dans le secteur privé, en particulier la notion de consentement, qui est la pierre angulaire de la LPRPDE.

Les renseignements personnels sont devenus une monnaie d'échange très recherchée, ce qui a entraîné la prolifération de nouvelles technologies et l'apparition de nouveaux modèles d'affaires. Dans ce marché de plus en plus complexe, bien des gens se demandent comment les Canadiens peuvent exercer en toute connaissance de cause leur droit de consentir à la collecte, à l'utilisation et à la communication de leurs renseignements personnels.

L'Internet des objets soulève des questions supplémentaires sur notre capacité, en tant qu'individus, à donner un consentement valable et éclairé. On est en voie de tout connecter à Internet – automobiles, réfrigérateurs, etc. Des capteurs recueillent constamment des données sur nos habitudes, et les organisations trouvent des façons d'analyser ces données et de les combiner avec celles générées par d'autres dispositifs dans notre maison et ailleurs. Ces renseignements offrent tellement de possibilités que les organisations peinent à expliquer leurs intentions. Elles n'en sont peut-être pas encore certaines elles-mêmes, ce qui ajoute à la complexité de l'obtention d'un consentement valable.

Nous avons récemment lancé un examen et une consultation sur la question fondamentale du consentement dans le monde numérique d'aujourd'hui. Nous espérons déterminer les améliorations qu'il serait possible d'apporter au modèle actuel et définir plus clairement le rôle et les responsabilités des divers acteurs qui pourraient les mettre en œuvre, soit les individus, les organisations, les organismes de réglementation et les législateurs. Nous apporterons ensuite les améliorations relevant de notre compétence et nous recommanderons au Parlement d'en apporter d'autres s'il y a lieu. Le présent rapport donne un aperçu du document de discussion que nous avons produit sur le sujet et de certaines solutions possibles.

La surveillance du gouvernement et le projet de loi C-51

Nous savons que les risques d'atteinte à notre sécurité sont réels et complexes. Les Canadiens veulent se sentir en sécurité, sans pour autant renoncer à leur droit à la vie privée. Ils souhaitent que les autorités adoptent une approche équilibrée et raisonnable. En ce qui a trait à cette priorité, notre objectif consiste à contribuer à l'adoption et à la mise en œuvre de lois et d'autres mesures protégeant à la fois la sécurité nationale et la vie privée.

Au cours du dernier exercice, nous avons contribué à l'élaboration, par Innovation, Sciences et Développement économique Canada, des lignes directrices sur les rapports de transparence destinées aux fournisseurs de services de télécommunications. Dans l'avenir, nous continuerons de réclamer l'élaboration de lignes directrices similaires applicables aux institutions fédérales.

Dans les mois précédant l'adoption du projet de loi C-51, *Loi antiterroriste de 2015*, j'ai formulé plusieurs observations au Parlement. J'ai alors expliqué en détail mes grandes inquiétudes concernant l'incidence de certaines

dispositions du projet de loi sur la protection de la vie privée. Malheureusement, le projet de loi a été adopté sans amendement.

Depuis l'adoption du projet de loi C-51, nous exerçons nos pouvoirs de vérification et d'examen pour déterminer comment se fait l'échange d'information entre des institutions fédérales dans la pratique, pour nous assurer que les nouvelles dispositions sont appliquées conformément à la *Loi sur la protection des renseignements personnels*. Le chapitre 2 brosse un tableau complet de la première phase de notre travail, au cours de laquelle nous avons mené un sondage auprès des institutions qui avaient déclaré avoir exercé les nouveaux pouvoirs d'échange de renseignements personnels que leur confère la Loi. Elles ont indiqué avoir communiqué des renseignements personnels à 58 reprises et en avoir reçu à 52 reprises. Selon elles, tous ces renseignements se rapportaient à des personnes soupçonnées de présenter une menace à la sécurité.

Pendant la prochaine phase de notre travail, nous examinerons et vérifierons les circonstances dans lesquelles se font ces échanges d'information. Notre objectif consiste à dresser un portrait aussi clair que possible du recours à la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et à d'autres lois afin d'informer le public et d'éclairer le débat qui se déroulera au Parlement au cours de l'examen du projet de loi C-51 que le gouvernement a annoncé. Nous espérons que cet examen aboutira à l'adoption de mesures qui protégeront efficacement la vie privée dans le contexte de la collecte et de l'échange d'information touchant la sécurité nationale.

Le chapitre 2 fait aussi état de notre examen de l'échange de métadonnées par le Centre de la sécurité des télécommunications (CST) avec ses partenaires du Groupe des cinq ainsi que de nos recommandations à cet égard. Après que le CST eut découvert qu'il communiquait davantage d'information sur les Canadiens que prévu en raison d'une défaillance technique, le ministre de la Défense nationale a mis le programme en veilleuse. Malgré tout, le CST a jugé que le risque d'atteinte à la vie privée était faible puisque l'information échangée était constituée uniquement de métadonnées, et non du contenu de communications, et que les partenaires du Groupe des cinq se sont engagés mutuellement à ne pas espionner les citoyens des autres pays du groupe. Nous avons soulevé des questions concernant cette évaluation, car nos recherches montrent que les métadonnées peuvent en fait constituer de l'information très sensible. Nous avons donc fait état dans nos recommandations de la nécessité de modifier la *Loi sur la défense nationale* afin qu'elle prévoie des garanties suffisantes pour protéger la vie privée des Canadiens.

La réputation et la protection de la vie privée

Les Canadiens sont conscients des avantages personnels et professionnels dont ils bénéficient en participant au monde numérique, mais ils s'inquiètent de plus en plus de leur réputation en ligne. Nous observons à cet égard de nouveaux problèmes d'atteinte à la vie privée dans les secteurs public et privé.

Suivant cette priorité stratégique, nous espérons aider à créer un environnement où les individus pourront se servir d'Internet afin d'explorer leurs intérêts et s'épanouir en tant qu'êtres humains sans craindre que les traces numériques de leurs activités ne leur fassent subir un traitement injuste.

En janvier 2016, nous avons diffusé un document de travail et sollicité des mémoires sur les enjeux liés à la vie privée touchant la réputation en ligne. Notre but était de définir une position concrète sur les mesures à prendre à l'égard de ces enjeux, notamment le droit à l'oubli. Nous souhaitons aussi aider à renseigner le public et à éclairer le débat au Parlement.

Le corps comme source d'information

La popularité croissante des accessoires intelligents à porter sur soi, comme les appareils de suivi de la condition physique, les vestes intelligentes et les autres produits connectés liés à la santé, ajoutent une dimension nouvelle et encore plus personnelle à l'Internet des objets.

Une industrie mondiale a vu le jour en exploitant l'information sur le corps humain. Certains appareils promettent des avantages réels pour les personnes et le système de santé dans son ensemble, mais les technologies utilisées pour extraire de l'information à même le corps humain et à son sujet véhiculent des renseignements personnels extrêmement sensibles.

... technologies utilisées pour extraire de l'information à même le corps humain et à son sujet véhiculent des renseignements personnels extrêmement **sensibles**.

Ce domaine connaît une croissance rapide. Or, on ne sait pas exactement si des mécanismes adéquats de protection des renseignements personnels sont toujours en place.

Nous voulons faire connaître les risques d'atteinte à la vie privée associés aux technologies conçues pour capter de l'information à même notre corps et à son sujet.

Nous voulons aussi faire des recherches et donner des orientations utiles dans ce domaine émergent. Dans un premier temps, nous avons analysé des applications et des technologies numériques existantes ou nouvelles dans le domaine de la santé, comme les appareils de suivi de la condition physique et les moniteurs de fréquence cardiaque. Nous prévoyons de tester certains de ces produits dans notre laboratoire de technologie pour mieux comprendre leurs répercussions sur la vie privée et renseigner les consommateurs en conséquence.

Rétrospective de l'exercice

Le dernier chapitre du rapport présente en détail tous les autres travaux importants réalisés par le Commissariat pour protéger et promouvoir le droit des individus à la vie privée au cours de la période couverte par le rapport.

Les nouvelles technologies et les nouveaux modèles d'affaires ont engendré des problèmes de protection de la vie privée qui n'avaient pas nécessairement été envisagés à l'époque de la conception de nos lois sur la protection des renseignements personnels ou qui remettent en question la pertinence des cadres actuels. De surcroît, le Commissariat s'est vu confier de nouvelles responsabilités qui sollicitent encore plus ses ressources et qui réduisent sa capacité à faire le travail proactif que nous estimons nécessaire.

Certes, l'établissement de nos priorités stratégiques nous a aidés à concentrer nos efforts sur les enjeux actuels et émergents et à adopter une approche stratégique aux fins de l'affectation de nos ressources.

Toutefois, le nombre d'atteintes à la vie privée déclarées au Commissariat augmente d'année en année, particulièrement depuis 2014, année où la politique du Conseil du Trésor a commencé à obliger les institutions fédérales à déclarer les atteintes substantielles. De plus, les organisations du secteur privé seront bientôt soumises à la même obligation en vertu du projet de loi S-4, *Loi sur la protection des renseignements personnels numériques*.

En dépit des défis à relever, nous nous efforçons de faire en sorte que les Canadiens bénéficient le plus possible de nos ressources et de nos outils. Par exemple, nous avons davantage recours à la procédure de règlement rapide des plaintes. À la lumière d'un examen diagnostic de nos activités en matière de conformité à la *Loi sur la protection des renseignements personnels*, nous mettons actuellement en œuvre un nouveau cadre de gestion des risques qui nous permettra d'accorder la priorité, dans nos enquêtes, aux dossiers susceptibles de porter le plus atteinte à la vie privée. En outre, nous collaborerons plus étroitement avec les institutions fédérales pour les aider à mieux se conformer à la Loi.

En parallèle, nous poursuivons nos efforts de sensibilisation du public pour aider les organisations et les individus à comprendre leurs droits et leurs responsabilités. Par exemple, l'an dernier, nous avons lancé de nouvelles stratégies pluriannuelles de sensibilisation ciblant les jeunes, les aînés et les petites entreprises. Nous savons que les personnes et les organisations se rendent très majoritairement en ligne pour se renseigner sur la protection de la vie privée, qu'il s'agisse de faire respecter leurs droits ou de s'acquitter de leurs responsabilités. C'est pourquoi nous nous sommes aussi efforcés de moderniser notre site Web pour bien répondre aux besoins des Canadiens.

Conscient que les questions de protection de la vie privée transcendent de plus en plus les frontières intérieures et internationales, le Commissariat continue de collaborer avec les organismes analogues des provinces, des territoires et des autres pays. Par exemple, au cours de la dernière année, nous avons collaboré avec les commissariats de l'Alberta et de la Colombie-Britannique pour donner de nouvelles orientations aux organisations sur la pratique consistant à permettre aux employés d'utiliser leurs propres appareils mobiles au travail et pour mettre à jour à leur intention une liste de vérification sur la sécurité en ligne.

Sur la scène internationale, nous avons coordonné les activités des 29 autorités de protection des données du monde entier qui ont participé à la troisième édition du ratissage international pour la protection de la vie privée, lequel portait sur les communications concernant la protection de la vie privée émanant des entreprises qui font du marketing en ligne auprès des enfants. Nous avons aussi coparrainé une résolution internationale qui a été adoptée à l'unanimité par les autorités de protection des données de partout dans le monde. Cette résolution avait pour but d'inciter les institutions gouvernementales à faire preuve d'une plus grande transparence concernant la collecte sans mandat de renseignements personnels des clients et des employés des organisations.

Conclusion

À mesure que les défis engendrés par les technologies du 21e siècle prennent de l'ampleur et que les modèles d'affaires évoluent, nous devons nous rendre à l'évidence : même en faisant tout notre possible pour réaliser des gains d'efficience et canaliser nos efforts, les outils à notre disposition pour protéger et promouvoir le droit des individus à la vie privée sont de plus en plus insuffisants.

... les outils à notre disposition pour **protéger et promouvoir le droit des individus à la vie privée** sont de plus en plus insuffisants.

Il faut apporter des modifications à la loi, aux cadres juridiques ainsi qu'aux pratiques des entreprises et des ministères et sensibiliser les gens afin que le Canada retrouve sa place comme chef de file de la protection de la vie privée et que les Canadiens en arrivent à exercer un meilleur contrôle sur leurs renseignements personnels.

La protection de la vie privée en chiffres

Demandes de renseignements liées à la LPRPDE*	**4 747**
Demandes de renseignements liées à la *Loi sur la protection des renseignements personnels*	**1 539**
Demandes de renseignements liées à aucune des deux lois	**3 810**
Plaintes en vertu de la LPRPDE acceptées*	**381**
Plaintes en vertu de la LPRPDE fermées à l'issue d'un règlement rapide*	**230**
Plaintes en vertu de la LPRPDE fermées à l'issue d'une enquête ordinaire*	**121**
Déclarations d'atteinte à la sécurité des données en vertu de la LPRPDE*	**115**
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées et traitées en vue d'une enquête	**1 389**
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées et mises en suspens	**379**
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* fermées à l'issue d'un règlement rapide	**460**
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* fermées à l'issue d'une enquête ordinaire	**766**
Déclarations d'atteinte à la sécurité des données en vertu de la *Loi sur la protection des renseignements personnels*	**298**
Évaluations des facteurs relatifs à la vie privée (EFVP) reçues	**88**
EFVP indiquant un « risque élevé »	**39**
EFVP indiquant un « risque faible »	**35**
Vérifications menées à bien dans le secteur public	**1**
Communications de renseignements dans l'intérêt public par les institutions fédérales	**441**
Lois et projets de loi examinés sous l'angle de leurs répercussions sur la protection de la vie privée (secteur privé)*	**1**
Comparutions devant des comités parlementaires sur des questions touchant le secteur privé*	**2**
Mémoires officiels présentés sur des questions touchant le secteur privé*	**3**
Autres interactions avec des parlementaires ou leur personnel (par exemple correspondance avec les bureaux des députés ou des sénateurs) sur des questions touchant le secteur privé*	**3**
Lois et projets de loi examinés sous l'angle de leurs répercussions sur la protection de la vie privée (secteur public)	**7**
Comparutions devant des comités parlementaires sur des questions touchant le secteur public	**6**
Mémoires officiels présentés sur des questions touchant le secteur public	**2**
Autres interactions avec des parlementaires ou leur personnel sur des questions touchant le secteur public	**3**
Allocutions prononcées et présentations données	**116**
Consultations du site Web principal	**1 819 835**
Consultations du blogue	**318 136**
Consultations du canal YouTube	**11 647**
Gazouillis envoyés	**650**
Abonnés sur Twitter le 31 mars 2016	**10 869**
Publications diffusées	**26 512**
News releases and announcements issued	**19**

* Statistiques se rapportant à la période comprise entre le 1er janvier 2015 et le 31 mars 2016. Les autres statistiques ont été recueillies au cours de la période comprise entre le 1er avril 2015 et le 31 mars 2016.

Chapitre 1 :

La réforme de la *Loi sur la protection des renseignements personnels*

La société canadienne et ses institutions fédérales ont connu des avancées technologiques majeures depuis 1983, année de l'entrée en vigueur de la *Loi sur la protection des renseignements personnels*. De plus en plus, la croissance fulgurante des technologies de l'information et des communications au cours des 30 dernières années a fait en sorte que les gouvernements peuvent recueillir et stocker les renseignements personnels de leurs citoyens beaucoup plus facilement et à un coût nettement moindre.

La *Loi sur la protection des renseignements personnels* est demeurée pratiquement inchangée, tandis que des lois similaires dans certaines provinces et à l'étranger en sont à la deuxième ou à la troisième génération.

La *Loi sur la protection des renseignements personnels* est demeurée pratiquement **inchangée** ...

On ne saurait trop insister sur l'importance de suivre le rythme de l'évolution des mesures de protection de la vie privée dans les autres pays, en particulier nos partenaires commerciaux et nos partenaires dans le domaine de la sécurité. Par exemple, au sein de l'Union européenne, les lois sur la protection des données interdisent la communication de renseignements personnels d'un pays membre vers un État l'étranger sauf si (entre autres exceptions) les mesures de protection des données et de la vie privée en vigueur dans le pays visé sont considérées comme « adéquates ».

Auparavant, l'examen du caractère adéquat de la protection offerte dans un pays étranger se limitait strictement à sa législation applicable au secteur privé. Mais des révélations survenues au cours des trois dernières années ont mis au jour un échange d'information considérable entre des organisations du secteur privé et des institutions gouvernementales, en particulier en Amérique du Nord. Ainsi, pour déterminer si la protection des renseignements personnels est adéquate dans un pays étranger, dorénavant l'Europe prendra en compte le cadre législatif global de ce pays en matière de vie privée, y compris ses dispositions concernant la sécurité nationale et les recours offerts aux ressortissants européens. Les responsables de l'Union européenne examineront attentivement ces normes au moment de se pencher sur le caractère adéquat des lois canadiennes.

Vers la fin du dernier exercice, le Parlement a pris une première mesure importante pour réformer nos lois dans le domaine de l'information, qui étaient à une époque les plus avancées dans le monde. Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels

et de l'éthique de la Chambre des communes examine actuellement la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*. En mars 2016, le Commissariat a témoigné devant le Comité et lui a alors présenté une lettre recommandant des modifications à apporter à la *Loi sur la protection des renseignements personnels*. Le Commissariat est bien placé pour alimenter le dialogue à ce sujet grâce aux connaissances pratiques acquises en interprétant et en appliquant la loi actuelle depuis plus de 30 ans. Il s'est lui-même heurté à toutes ses limites.

Comment faire entrer la *Loi sur la protection des renseignements personnels* dans le 21e siècle

Notre lettre concernant la modernisation de la *Loi sur la protection des renseignements personnels* renfermait 16 recommandations axées sur trois grands thèmes : les changements technologiques, la modernisation des normes juridiques et l'accroissement de la transparence.

LES CHANGEMENTS TECHNOLOGIQUES

En raison des changements technologiques, les gouvernements ont pu augmenter de manière exponentielle la quantité d'information qu'ils recueillent, stockent et communiquent. Les règles de droit en vigueur ne suffisent tout simplement pas pour régir ce type d'échange massif de données ou garantir que les renseignements personnels détenus par les institutions fédérales sont protégés adéquatement contre toute communication non autorisée. Le débat public souvent passionné dont a fait l'objet le projet de loi C-51, *Loi antiterroriste de 2015* (voir le chapitre 2), montre bien que le sujet intéresse beaucoup de Canadiens. Cette loi autorise un échange encore plus large de renseignements personnels entre les ministères et organismes fédéraux.

La communication des renseignements personnels devrait faire l'objet d'ententes écrites

Sous sa forme actuelle, la *Loi sur la protection des renseignements personnels* autorise les institutions fédérales à communiquer les renseignements personnels qu'elles détiennent à d'autres institutions fédérales, aux autorités provinciales ou à des États étrangers pour diverses raisons, notamment pour un « usage compatible avec les fins auxquelles les renseignements ont été recueillis ». Or, d'après notre expérience et compte tenu du libellé actuel, les institutions fédérales font valoir depuis longtemps une interprétation très large du concept d'« usage compatible » inscrit dans la Loi.

Nous avons recommandé de modifier la *Loi sur la protection des renseignements personnels* pour obliger les institutions fédérales à conclure des ententes écrites avant de communiquer des renseignements personnels. Entre autres, ces ententes indiqueraient la fin à laquelle les renseignements sont communiqués; limiteraient les utilisations des renseignements personnels à une fin secondaire et tout transfert ultérieur; et mentionneraient les autres mesures à prévoir dans la réglementation, comme les mesures de protection particulières, les périodes de conservation et les mesures de reddition de comptes. Mais surtout, les ententes écrites seraient, pour les Canadiens, un gage de transparence en expliquant l'utilisation que font les institutions fédérales de leurs renseignements personnels. Nous avons aussi recommandé aux décideurs de conférer au Commissariat le pouvoir d'examiner les ententes, de les commenter et de déterminer si elles sont respectées.

La loi doit rendre obligatoire la protection des renseignements personnels

Les centaines d'atteintes à la sécurité des données dans les institutions fédérales déclarées au Commissariat indiquent un manque de mesures de protection adéquates. En raison des progrès technologiques, les institutions fédérales recueillent et utilisent des quantités de renseignements personnels qui ne cessent de croître, sans nécessairement avoir mis en place des mesures de protection adéquates. Le risque d'atteinte à la sécurité des données et les conséquences susceptibles d'en découler s'en trouvent accrus.

Au fil des ans, des atteintes massives à la sécurité des données du gouvernement ont touché des dizaines, voire des centaines de milliers de personnes. Par exemple en 2012, le ministère qui s'appelait alors Ressources humaines et du Développement des compétences Canada a signalé la perte d'un disque dur externe renfermant les renseignements personnels de près de 600 000 personnes ayant participé au Programme canadien de prêts aux étudiants – nom, date de naissance, numéro d'assurance sociale, adresse, numéro de téléphone et renseignements financiers.

… la *Loi sur la protection des renseignements personnels* n'oblige pas expressément ces institutions à **protéger** les renseignements personnels qu'elles détiennent.

Étonnamment, compte tenu de la grande quantité de renseignements personnels que les citoyens ont l'obligation de communiquer à des ministères et organismes fédéraux, la *Loi sur la protection des renseignements personnels* n'oblige pas expressément ces institutions à protéger les renseignements personnels qu'elles détiennent. Pourtant, la protection des données est un principe universel qui revient dans la plupart des lois sur la protection des renseignements personnels dans le monde, y compris la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Nous estimons que ce type de protection devrait figurer aussi dans la *Loi sur la protection des renseignements personnels*.

Dans certains cas, d'importantes atteintes à la sécurité des renseignements personnels n'ont même pas été déclarées au Commissariat. En 2013, Santé Canada a envoyé à plus de 41 000 personnes partout au pays des lettres insérées dans des enveloppes à fenêtre montrant non seulement le nom et l'adresse du destinataire, mais aussi une mention révélant que l'expéditeur était le Programme d'accès à la marijuana à des fins médicales. Or, Santé Canada n'a pas déclaré cette atteinte à la sécurité des données. Plusieurs centaines de personnes ayant reçu ces lettres étaient d'un tout autre avis et se sont plaintes au Commissariat que le Ministère avait révélé des renseignements personnels sensibles sans leur consentement.

Aujourd'hui, la politique du Secrétariat du Conseil du Trésor du Canada oblige les institutions fédérales à déclarer au Commissariat toute atteinte « substantielle » à la sécurité des renseignements personnels. En 2015-2016, soit le deuxième exercice complet où les institutions fédérales étaient soumises à cette obligation, 298 atteintes nous ont été signalées, soit une augmentation par rapport aux 256 de l'exercice précédent et aux 109 de 2012-2013, dernier exercice au cours duquel

la déclaration se faisait sur une base volontaire. Il est grand temps d'imposer dans une loi cette obligation qui n'est prévue pour l'instant que dans une politique. Le Commissariat aurait ainsi une meilleure idée de l'ampleur actuelle du problème et il serait consulté dans le cadre de la démarche visant à remédier aux atteintes et à atténuer leurs répercussions sur les individus.

Ce changement empêcherait le décalage en voie de se créer entre la loi canadienne applicable au secteur public fédéral et celle qui s'applique au secteur privé. En vertu des modifications récemment apportées à la LPRPDE, les organisations du secteur privé seront tenues de déclarer les atteintes à la sécurité des renseignements personnels. Ce type d'obligation, qui figure dans de nombreuses lois modernes, est imposé depuis 2013 dans la version révisée des *Lignes directrices régissant la protection de la vie privée* publiée par l'Organisation de coopération et de développement économiques (OCDE).

LA MODERNISATION DES NORMES JURIDIQUES

Le passage du papier aux supports informatiques a entraîné une collecte excessive de renseignements. L'appétit des institutions fédérales pour les renseignements personnels de la population a crû en corrélation directe avec la facilité avec laquelle il était possible de les recueillir. Nous avons observé cette tendance dans de nombreux programmes. La première mesure que nous avons recommandée pour éviter dans l'avenir un décalage considérable entre la *Loi sur la protection des renseignements personnels* et le monde réel consiste à imposer un examen de cette loi par le Parlement tous les cinq ans.

Il faut limiter la collecte aux renseignements nécessaires

En vertu de la *Loi sur la protection des renseignements personnels*, « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ». Selon notre interprétation, cette disposition devrait signifier que la collecte des renseignements doit être nécessaire à un programme ou à une activité. Cette interprétation est conforme à la *Directive sur les pratiques relatives à la protection de la vie privée* du SCT. Il s'agit aussi d'un facteur important que devrait mesurer l'Union européenne pour trancher la question du caractère adéquat.

Cependant, notre interprétation n'est pas retenue uniformément dans l'ensemble du gouvernement. De fait, dans un mémoire déposé récemment, la procureure générale du Canada a rejeté explicitement l'utilisation du critère de nécessité comme seuil pour la collecte de renseignements personnels en vertu de la loi. Elle a préconisé une interprétation plus large de l'expression « lien direct » qui permettrait une collecte plus importante de renseignements personnels. La Cour fédérale du Canada n'a pas encore rendu sa décision dans cette affaire.

De plus, le Secrétariat du Conseil du Trésor a modifié récemment la *Norme sur le filtrage de sécurité* afin d'autoriser une collecte de renseignements personnels beaucoup plus étendue que par le passé. Le Commissariat a été autorisé à intervenir dans une contestation judiciaire de la nouvelle version de la norme par le Syndicat des agents correctionnels du Canada. Nous interviendrons à titre de partie neutre pour aider le tribunal à interpréter l'article en question de la *Loi sur la protection*

des renseignements personnels. En outre, nous nous sommes penchés sur l'évaluation par le Secrétariat du Conseil du Trésor des répercussions de la nouvelle norme sur la vie privée et nous examinons actuellement plusieurs plaintes liées à cette question.

Des mesures de protection des renseignements personnels doivent être prises dès le départ pour prévenir les risques d'atteinte à la vie privée

Le Secrétariat du Conseil du Trésor a publié la *Directive sur l'*évaluation des facteurs relatifs à la vie privée pour permettre de cerner, d'évaluer et d'atténuer de façon appropriée les risques d'atteinte à la vie privée avant de mettre en œuvre une activité ou un programme nouveau ou ayant subi des modifications importantes. Cette directive demande aux institutions fédérales de présenter leurs évaluations au Commissariat aux fins d'examen et de commentaires. Nous avons constaté que cette façon de procéder est très utile pour cerner et atténuer les risques d'atteinte à la vie privée avant la mise en œuvre du programme ou de l'activité. Des institutions fédérales nous l'ont aussi souligné. Toutefois, cette politique n'a pas force de loi. C'est pourquoi la pratique, la qualité et le caractère opportun varient parfois grandement d'une institution fédérale à l'autre. Certaines institutions qui traitent de grandes quantités de renseignements personnels sensibles présentent rarement au Commissariat des évaluations des facteurs relatifs à la vie privée (EFVP).

De même, certaines institutions fédérales peuvent décider de n'effectuer aucune EFVP dans des situations où, d'après nous, ce serait manifestement nécessaire. Il arrive aussi qu'elles effectuent leur évaluation très tard dans le processus de mise en œuvre du nouveau programme. Par exemple, l'Agence des services frontaliers du Canada n'a pas consulté le Commissariat en 2013 avant de mettre en œuvre sa *Norme d'intégrité élevée pour les enquêtes de sécurité sur le personnel* et elle a produit une EFVP uniquement au moment de sa mise en œuvre. L'Agence a donc commencé, sans attendre notre avis, à mettre en place de nouveaux contrôles plus envahissants pour ses enquêtes de sécurité, pratique qui a donné lieu au dépôt d'une plainte en vertu de la *Loi sur la protection des renseignements personnels*. Si la loi obligeait les institutions fédérales à effectuer une EFVP avant de mettre en œuvre un programme, les risques d'atteinte à la vie privée pourraient être mis en évidence et atténués dès le début.

L'examen des plaintes et les procédures judiciaires prennent beaucoup de temps et coûtent cher. On pourrait les éviter si la loi obligeait les institutions fédérales à réaliser des EFVP avant de lancer un programme présentant des risques particuliers. Depuis des années, nous ne cessons de souligner à quel point il est plus efficace et moins coûteux de cerner et de maîtriser les risques d'atteinte à la vie privée au cours de la conception d'un programme que d'avoir à le modifier après sa mise en œuvre.

De plus, afin de détecter les écueils sur le front de la protection de la vie privée avant qu'ils deviennent des problèmes réels, nous avons recommandé de modifier la *Loi sur la protection des renseignements personnels* pour qu'elle oblige les institutions fédérales à consulter le Commissariat sur leurs avant-projets de loi ou de règlement susceptibles d'avoir des répercussions sur la vie privée. Des provinces canadiennes et d'autre pays imposent déjà cette obligation.

Enfin, le Commissariat serait mieux en mesure de poursuivre les objectifs de la *Loi sur la protection des renseignements personnels* si celle-ci lui conférait explicitement le mandat de faire de la sensibilisation et de la recherche. La LPRPDE lui confère un mandat similaire, qui s'est avéré très bénéfique.

L'ACCROISSEMENT DE LA TRANSPARENCE

Les dispositions de la *Loi sur la protection des renseignements personnels* régissant la confidentialité ne nous permettent actuellement de rendre publiques les conclusions de nos enquêtes que dans le cadre des rapports annuels et des rapports spéciaux que nous présentons au Parlement. Nous reconnaissons que l'application de ces dispositions est raisonnable dans la plupart des cas, mais la *Loi sur la protection des renseignements personnels* devrait prévoir, à l'instar de la LPRPDE, certaines exceptions pour des raisons d'intérêt public. Cette latitude devrait avoir comme principal objectif de nous permettre d'éclairer en temps opportun le débat au sein du Parlement et de la société en général.

La nécessité d'accroître la transparence nous semble particulièrement manifeste dans le contexte de **l'application de la loi**.

Dans le passé, les contraintes de confidentialité imposées dans la *Loi sur la protection des renseignements personnels* ont entravé la capacité du Commissariat d'éclairer le débat et les discussions. Par exemple, dans le cas de la participation de l'Agence des services frontaliers du Canada à une émission de télévision (voir le chapitre 6) et dans celui de la collecte, par des ministères, de renseignements personnels concernant une militante défendant les droits des Premières Nations sur sa page personnelle dans un réseau social (voir notre rapport annuel 2012-2013), nous n'avons pu diffuser publiquement nos conclusions avant de déposer notre rapport au Parlement plusieurs mois plus tard.

Par souci de transparence, nous avons aussi recommandé que les ministères soient tenus de rendre compte, de manière plus compréhensible, de leur administration de *Loi sur la protection des renseignements personnels*. Ces rapports des ministères présentent habituellement une panoplie de statistiques sur le nombre de demandes de renseignements personnels reçues ou traitées au cours d'un exercice, mais on n'y trouve guère d'explications sur la signification de ces statistiques. Afin que ces rapports soient révélateurs et utiles pour les besoins de la transparence, on doit pouvoir les comprendre.

La nécessité d'accroître la transparence nous semble particulièrement manifeste dans le contexte de l'application de la loi. Nous avons exhorté les organisations fédérales à communiquer ouvertement le nombre de demandes d'accès licite à des renseignements personnels qu'ils adressent à des fournisseurs d'accès Internet et à d'autres organisations du secteur privé auxquels sont confiés des renseignements des clients en précisant la fréquence et la nature de ces demandes. Au Canada, le public, les parlementaires et le milieu de la protection de la vie privée réclament depuis plusieurs années une transparence accrue à cet égard.

Les individus doivent avoir le meilleur accès possible à leurs renseignements personnels

Pour favoriser la transparence et respecter le principe du gouvernement ouvert, il est important de permettre aux individus d'avoir accès aux renseignements personnels les

concernant que détiennent les institutions fédérales. Nous avons recommandé d'accorder aux ressortissants étrangers le droit d'accès à leurs renseignements personnels et d'assurer une communication maximale, s'il y a lieu, lorsque des individus demandent à avoir accès aux renseignements personnels les concernant.

Pour ce faire, il faut limiter les exceptions prévues dans la *Loi sur la protection des renseignements personnels*, s'assurer que ces exceptions seront généralement discrétionnaires et fondées sur le préjudice, s'il y a lieu, et, dans la mesure du possible, retrancher l'information protégée.

La Loi sur la protection des renseignements personnels *devrait s'appliquer à toutes les institutions fédérales.*

La *Loi sur la protection des renseignements personnels* devrait s'appliquer à toutes les institutions fédérales.

Nous estimons que, par principe, les individus devraient avoir accès à leurs renseignements personnels et pouvoir en contester l'exactitude, quelle que soit l'institution fédérale qui les détient.

Cet accès serait d'ailleurs conforme à l'un des objectifs fondamentaux visés par la désignation des agents du Parlement, à savoir donner aux citoyens un aperçu des activités du pouvoir exécutif.

Le commissaire devrait avoir le pouvoir de communiquer de l'information pour faire respecter la loi

Plus que jamais, on peut dire que les renseignements personnels transcendent les frontières, en particulier dans un monde exposé à des menaces à la sécurité mondiale. À la suite de modifications récentes, la LPRPDE confère explicitement au Commissariat le pouvoir d'échanger des renseignements avec des organismes analogues au pays et à l'étranger pour faciliter la collaboration en matière d'application de la loi dans le secteur privé. Nous avons recommandé de conférer explicitement au Commissariat un pouvoir similaire de collaborer avec les autres autorités de protection des données et les organismes d'examen à l'échelle nationale et internationale dans le cadre des vérifications et des enquêtes qui portent sur des questions d'intérêt commun touchant la *Loi sur la protection des renseignements personnels*.

Conclusion

Les Canadiens s'attendent désormais à ce que le gouvernement fasse preuve d'une ouverture et d'une transparence accrues en indiquant à quelles fins il utilisera leurs renseignements personnels, à qui il les communiquera et comment il les protégera. À l'échelle nationale et internationale, les lois sur la protection des renseignements personnels ont fait avancer les choses considérablement depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983. Sous sa forme actuelle, cette loi offre une protection qui est de plus en plus en décalage avec les Canadiens et leurs activités dans un monde numérique.

Nous estimons que la modernisation de la *Loi sur la protection des renseignements personnels* assurerait la protection et le droit à la vie privée auxquels s'attendent les Canadiens et qui refléteraient les réalités technologiques, l'expérience et le courant de pensée actuels au Canada et ailleurs dans le monde.

Nous sommes impatients de poursuivre la discussion avec le Parlement concernant la modernisation de la *Loi sur la protection des renseignements personnels* pour l'adapter aux réalités du 21e siècle.

Chapitre 2 :

Le projet de loi C-51 et la surveillance du gouvernement

Le Canada n'est pas le seul pays en quête des moyens les plus efficaces pour protéger ses citoyens contre les menaces à la sécurité nationale. Partout dans le monde, les gouvernements recueillent et communiquent de plus en plus de renseignements personnels dans le but de détecter et de prévenir les menaces. Grâce aux nouvelles technologies, il est maintenant possible de recueillir et d'analyser des quantités de données auparavant inimaginables. Dans notre société démocratique, il est essentiel de trouver le juste équilibre entre le besoin de sécurité et le respect de la vie privée. Les institutions fédérales ayant comme mandat d'assurer la sécurité doivent être en mesure de protéger les Canadiens, mais elles doivent exercer leurs activités dans le respect de la primauté du droit.

Nous devons déterminer si les mesures de protection de la vie privée **conçues au début des années 1980** sont encore adéquates en cette ère nouvelle.

Lorsque nous avons consulté les Canadiens pour établir nos priorités, ils ont été nombreux à soulever la question des pouvoirs et des moyens sans cesse plus importants dont disposent les organismes gouvernementaux pour recueillir et communiquer des renseignements personnels à leur sujet.

Les personnes que nous avons consultées comprennent l'importance de la surveillance pour assurer la sécurité nationale et prévenir le crime, mais elles remettent en question la façon dont la surveillance et l'établissement de profils de risque à leur insu pourraient porter atteinte aux libertés et aux droits fondamentaux. Elles ont également réclamé une plus grande transparence.

Le débat national ayant suivi le dépôt du projet de loi C-51, *Loi antiterroriste de 2015*, en janvier 2015 a mis en évidence l'ampleur des préoccupations à cet égard. Cette loi et d'autres lois qui confèrent aux ministères et organismes gouvernementaux des pouvoirs nouveaux et élargis de recueillir et de communiquer de l'information menacent sérieusement notre cadre actuel de protection de la vie privée.

Nous devons déterminer si les mesures de protection de la vie privée conçues au début des années 1980 sont encore adéquates en cette ère nouvelle. L'objectif ultime que nous nous sommes fixé en ce qui a trait à la surveillance du gouvernement – une de nos priorités stratégiques liées la vie privée – est de contribuer à l'adoption et à l'application de lois et d'autres mesures qui ont manifestement pour effet d'assurer la sécurité nationale et de protéger la vie privée.

Le projet de loi C-51, *Loi antiterroriste de 2015*

Le projet de loi C-51 a reçu la sanction royale en juin 2015 et la *Loi antiterroriste de*

2015 est entrée en vigueur en août 2015. La nouvelle loi édicte la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), à l'égard de laquelle le Commissariat a exprimé de sérieuses préoccupations dans les mémoires qu'il a présentés à plusieurs comités parlementaires ayant examiné le projet de loi, y compris le Comité sénatorial permanent de la sécurité nationale et de la défense.

Depuis, un nouveau gouvernement a été porté au pouvoir et il s'est engagé à tenir des consultations sur les modifications à apporter à la LCISC. Le Commissariat serait heureux d'avoir la possibilité d'exprimer son point de vue dans ce contexte.

Le Commissariat a accueilli favorablement le projet de loi visant à créer un comité parlementaire chargé de surveiller les activités de l'État liées à la sécurité nationale. Il s'agit selon nous d'un premier pas dans la bonne direction. Cependant, nous avons aussi recommandé que les institutions autorisées à recevoir de l'information aux fins de la sécurité nationale soient soumises à une supervision, à des examens par des experts ou à des examens administratifs indépendants.

La question de la surveillance des activités de sécurité est en partie réglée, mais les seuils établis pour la communication d'information continuent de nous préoccuper. Selon la norme actuelle définie dans la LCISC, certaines institutions fédérales peuvent échanger des renseignements entre elles, pourvu que ces renseignements soient « pertinents » aux fins de la détection de menaces à la sécurité nationale. Ce seuil nous semble inadéquat et il pourrait donner accès aux renseignements personnels de citoyens respectueux des lois. Il serait plus raisonnable de retenir comme seuil le critère de la « nécessité » pour autoriser la communication des renseignements personnels.

Dans le cadre de notre priorité stratégique portant sur la surveillance du gouvernement, nous avons prévu plusieurs mesures à court et à moyen terme pour réduire les risques d'atteinte à la vie privée pouvant découler de la LCISC. Nous nous sommes aussi engagés à examiner la mise en œuvre des lois sur la sécurité nationale, comme le projet de loi C-51, pour assurer la conformité à la *Loi sur la protection des renseignements personnels*. Nous présenterons des rapports à cet égard dans le but d'éclairer le débat public.

Nous avons déclaré que nous publierions nos conclusions à l'intention des parlementaires et du public et que nous formulerions des recommandations en vue d'améliorer les politiques ou les lois au besoin.

Nous tenons cet engagement. Nous avons récemment examiné la façon dont la LCISC a été mise en œuvre et appliquée au cours des six premiers mois. Nous avons soulevé plusieurs préoccupations et formulé des recommandations.

EXAMEN DE LA FAÇON DONT LA *LOI SUR LA COMMUNICATION D'INFORMATION AYANT TRAIT À LA SÉCURITÉ DU CANADA* A ÉTÉ MISE EN ŒUVRE ET APPLIQUÉE AU COURS DES SIX PREMIERS MOIS

1. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) est entrée en vigueur le 1er août 2015. Elle a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication afin de protéger le pays contre des « activités portant atteinte à la sécurité du Canada ». En déposant le projet de loi, le gouvernement a déclaré que la communication d'information efficiente, efficace et responsable entre les diverses institutions fédérales est de plus en plus essentielle pour cerner, comprendre et contrer les menaces à la sécurité nationale. En vertu de la Loi, l'information peut être communiquée si elle se rapporte au mandat ou aux attributions de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité nationale, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention, l'enquête ou la perturbation de ces activités ou une enquête sur celles-ci. Il est important de protéger la sécurité des Canadiens. Et nous sommes conscients qu'une communication accrue de l'information peut aider à cerner et à éliminer les menaces à la sécurité.

2. La LCISC est formulée en termes généraux et laisse beaucoup de latitude aux institutions fédérales pour interpréter et définir les « activités portant atteinte à la sécurité du Canada », ce qui pourrait entraîner un manque d'uniformité dans son application. De plus, l'ampleur éventuelle de la communication d'information en vertu de cette loi atteint des proportions sans précédent. Un examen préliminaire des données semble indiquer un recours limité à la LCISC pendant les six premiers mois de sa mise en œuvre, mais la possibilité d'une communication à une échelle beaucoup plus grande, combinée aux progrès technologiques, permettrait d'analyser les renseignements personnels au moyen d'algorithmes pour déceler des tendances et prévoir le comportement. Des Canadiens ordinaires pourraient ainsi faire l'objet d'un profilage visant à repérer parmi eux des individus menaçant la sécurité. Dans nos futurs examens, nous tenterons de déterminer si ces vastes pouvoirs de communication d'information touchent effectivement des citoyens respectueux des lois et, le cas échéant, dans quelles situations.

3. Certaines institutions fédérales responsables de la sécurité nationale font actuellement l'objet d'examen ou de surveillance dans une certaine mesure. Toutefois, 14 des 17 institutions autorisées en vertu de la LCISC à recevoir de l'information aux fins de la sécurité nationale ne font l'objet d'aucun examen indépendant ni d'aucune surveillance. Soulignons que le gouvernement a annoncé

son intention de créer un comité parlementaire chargé des questions de sécurité nationale.

4. Nous avons amorcé un examen pour informer les intervenants, notamment les parlementaires, de l'ampleur de la communication d'information en vertu de LCISC. Nous avons aussi mené un sondage auprès de 128 institutions fédérales, soit les 17 institutions autorisées à recueillir et à communiquer de l'information en vertu de cette loi et les 111 institutions fédérales désormais autorisées à leur communiquer de l'information. Le sondage portait sur les six premiers mois suivant l'entrée en vigueur de la LCISC, soit du 1er août 2015 au 31 janvier 2016.

5. Selon le sondage, cinq institutions ont déclaré avoir recueilli ou communiqué de l'information en vertu de la LCISC au cours des six premiers mois suivant son entrée en vigueur. L'Agence des services frontaliers du Canada, la Gendarmerie royale du Canada, Immigration, Réfugiés et Citoyenneté Canada ainsi que le Service canadien du renseignement de sécurité ont affirmé avoir reçu (c'est-à-dire recueilli) de l'information en vertu de la Loi à 52 reprises au total. Affaires mondiales Canada, l'Agence des services frontaliers du Canada et Immigration, Réfugiés et Citoyenneté Canada ont déclaré avoir communiqué de l'information en vertu de la LCISC à 58 reprises au total au cours de cette période. Les 111 autres institutions fédérales sondées ont indiqué n'avoir communiqué aucune information en vertu de la Loi. Le sondage comportait aussi des questions d'ordre général sur la nature des activités de communication d'information. Ces questions avaient pour but d'avoir une idée du risque pour les citoyens respectueux des lois. Nous avons demandé aux institutions sondées si l'information communiquée se rapportait à des individus en particulier ou à des catégories d'individus. Nous voulions aussi savoir si cette information portait sur des personnes qui n'étaient pas soupçonnées de porter atteinte à la sécurité du Canada au moment de la communication. D'après les répondants, l'information communiquée en vertu de la LCISC se rapportait à des individus nommément désignés et soupçonnés de porter atteinte à la sécurité du Canada.

6. Avant l'adoption de la LCISC, d'autres lois autorisaient déjà la collecte et la communication d'information aux fins de la sécurité nationale. Certains pouvoirs sont aussi assez vastes, y compris les pouvoirs conférés aux services policiers et à d'autres en vertu de la common law et la prérogative de la Couronne pour la défense. Selon le sondage, 13 des 17 institutions fédérales avaient exercé les pouvoirs préexistants pour recueillir ou communiquer de l'information. Nous n'avons pas cherché à connaître l'ampleur de l'information communiquée; toutefois, neuf institutions ont confirmé que

l'information concernait des individus en particulier.

7. Sécurité publique Canada est responsable de toutes les questions ayant trait à la sécurité publique et à la gestion des urgences qui ne relèvent d'aucune autre institution fédérale. Ce ministère est également chargé de coordonner les activités des entités au sein du portefeuille de la Sécurité publique, notamment la Gendarmerie royale du Canada, le Service canadien du renseignement de sécurité et l'Agence des services frontaliers du Canada. La Loi autorise le gouverneur en conseil, sur recommandation du ministre de la Sécurité publique et de la Protection civile, à prendre des règlements pour la mise en œuvre de la LCISC, notamment au sujet de la communication d'information ainsi que des exigences en matière de tenue et de conservation de documents imposées par la Loi. Toutefois, il ne l'a pas encore fait.

8. Pour appuyer la mise en œuvre de la LCISC, Sécurité publique Canada a préparé un document d'orientation à l'intention des employés des institutions fédérales ainsi que le document intitulé Loi sur la communication d'information ayant trait à la sécurité du Canada : Cadre public, que les Canadiens peuvent consulter. Nous avons étudié ces documents dans le cadre de notre examen. Ils préconisent généralement un échange d'information responsable, mais ils manquent de précisions et de détails concernant les moyens que devraient prendre les ministères et organismes fédéraux pour atteindre cet objectif tout en respectant la vie privée. Plus précisément, nous avons constaté qu'il manque les éléments suivants dans le document d'orientation :

- des orientations faisant état de la nécessité de conclure des ententes d'échange d'information et indiquant les éléments de base qu'elles devraient contenir;
- des explications et des exemples suffisants, y compris des scénarios, établissant les seuils pour la communication et l'utilisation d'information en vertu de la LCISC;
- des orientations sur l'importance de prévenir la communication de renseignements personnels par inadvertance au cours de discussions entre l'institution qui communique l'information et celle qui la reçoit;
- une explication des facteurs qui limiteraient la communication d'information;
- des orientations sur le contenu des documents qui devraient être conservés, notamment une description de l'information communiquée et le motif de la communication;

- des orientations sur la destruction ou le renvoi d'information dont la loi n'autorise pas la collecte.

9. La *Directive sur l'*évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (SCT), qui est entrée en vigueur en 2010, vise à s'assurer que la protection des renseignements personnels constitue un élément central de l'élaboration initiale et de l'administration subséquente des programmes et des activités nécessitant la collecte de renseignements personnels. Elle a été publiée en partie en réponse aux Canadiens et aux parlementaires qui avaient exprimé des préoccupations concernant les répercussions complexes et délicates, sur la vie privée, des mesures antiterroristes proactives, du recours à la surveillance et à des technologies portant atteinte à la vie privée, des échanges transfrontaliers de renseignements personnels et des atteintes à la sécurité menaçant le droit à la vie privée.

10. Nous avons examiné le document d'orientation de Sécurité publique Canada pour déterminer s'il donnait des orientations claires concernant l'obligation de réaliser une évaluation des facteurs à la vie privée (EFVP) avant de recueillir ou de communiquer de l'information en vertu de la LCISC. Selon ce document, il ne devrait pas être nécessaire de modifier une EFVP à moins que certains éléments déclencheurs habituels ne soient présents. Les pouvoirs de recueillir l'information peuvent demeurer inchangés pour les institutions qui reçoivent de l'information en vertu de la LCISC, mais cette loi vise manifestement à accroître la quantité et la diversité de l'information pouvant être reçue par rapport à la situation avant son adoption. La communication d'information à des fins autres que celles prévues au moment de la collecte constitue une modification importante à un programme ou à une activité de l'institution. Selon *la Directive sur l'*évaluation des facteurs relatifs à la vie privée, ce type de modification devrait donner lieu à une EFVP nouvelle ou modifiée. Les orientations relatives aux EFVP données dans le document d'orientation de Sécurité publique Canada devraient concorder avec les exigences et l'intention de la directive du SCT.

11. Douze (12) des 17 institutions fédérales autorisées à recueillir de l'information en vertu de la LCISC ont effectué une analyse quelconque pour déterminer s'il était nécessaire d'effectuer une EFVP relativement à leurs processus d'échange d'information. Deux d'entre elles ont estimé que cette évaluation s'imposait et elles la préparent à l'heure actuelle.

12. Dans le cadre de notre sondage, nous avons demandé aux institutions si elles s'étaient dotées d'une politique ou d'un document d'orientation pour donner effet à la LCISC. Comme nous l'avons déjà indiqué, cinq institutions avaient recueilli ou communiqué des

renseignements personnels en vertu de cette loi au cours de la période visée par l'examen, dont trois s'étaient dotées d'une politique ou d'un document d'orientation. L'examen de ces documents nous a permis de constater qu'ils manquent de précisions et de détails pour être vraiment utiles aux employés lorsqu'il s'agit de déterminer si les seuils prévus par la LCISC ont été atteints. Ce petit échantillon fait ressortir l'importance d'établir des orientations pangouvernementales claires pour ce qui est de donner effet à cette loi.

13. **Recommandation :** Sécurité publique Canada devrait donner aux institutions fédérales des orientations et des lignes directrices suffisantes pour s'assurer que :

    - les institutions concluent des ententes d'échange d'information renfermant les dispositions essentielles sur la protection de la vie privée;
    - le personnel comprend les seuils pour la collecte ou la communication d'information en vertu de la LCISC;
    - les discussions entre l'institution qui communique de l'information et celle qui la reçoit ne donnent pas lieu à la communication de renseignements personnels par inadvertance;
    - les facteurs qui limiteraient la communication d'information sont expliqués;
    - des pratiques adéquates de tenue de documents sont en place;
    - les répercussions sur la vie privée des activités de collecte et de communication d'information en vertu de la LCISC sont évaluées;
    - tout renseignement qu'une institution ne peut pas recueillir de façon licite est immédiatement détruit ou renvoyé à l'institution d'origine.

Réponse du Ministère : *Sécurité publique Canada est d'accord avec la recommandation.*

Sécurité publique Canada a déjà donné des orientations aux institutions concernant la Loi sur la communication d'information ayant trait à la sécurité du Canada *(LCISC) et il continuera de le faire. Par exemple, le ministère de la Sécurité publique donnera des orientations supplémentaires sur les pratiques appropriées pour la tenue de documents, les seuils pour la communication, l'obligation de détruire ou de renvoyer immédiatement à l'expéditeur toute information qu'une institution n'est pas autorisée à recueillir en vertu de la loi ainsi que sur les*

autres questions mentionnées dans la recommandation.

La Loi sur le ministère de la Sécurité publique et de la Protection civile *confère au ministre et, par le fait m*ême, au *ministère le pouvoir de « coordonner, mettre en œuvre et promouvoir des politiques, projets et programmes en matière de sécurité publique et de protection civile » et de « faciliter le partage de l'information – s'il y est autorisé – en vue de promouvoir les objectifs liés à la sécurité publique ». Conformément à ce mandat, les orientations élaborées par Sécurité publique Canada concernant la LCISC et les pouvoirs de communication d'information qu'elle confère sont donnés aux institutions pour les aider à comprendre cette loi. Il incombe à l'administrateur général de veiller à ce que cette loi soit respectée au sein de son institution.*

14. Au cours de la prochaine phase de notre examen, nous nous attacherons à vérifier les détails et la nature des échanges de renseignements personnels en vertu de la LCISC, notamment pour confirmer les renseignements que nous donnent les ministères. Nous examinerons aussi les échanges de renseignements personnels – aux fins de la sécurité nationale – qui se font en vertu de pouvoirs conférés par d'autres lois. Nous voulons ainsi brosser un tableau aussi clair que possible du recours aux pouvoirs conférés par la LCISC et à d'autres pouvoirs pour éclairer le débat public et celui qui aura lieu au Parlement dans le cadre de l'examen du projet de loi C-51 qu'a annoncé le gouvernement. Nous espérons que notre travail dans ce domaine conduira à l'adoption de mesures qui protègent efficacement la vie privée dans le cadre de la collecte et de la communication d'information touchant la sécurité nationale.

Les activités de la prochaine phase de l'examen commenceront en 2016-2017.

La communication de métadonnées par des organismes de sécurité donne lieu à un examen et à des recommandations du Commissariat.

En janvier 2016, le ministre de la Défense nationale a annoncé que, jusqu'à nouvel ordre, le Centre de la sécurité des télécommunications (CST) ne communiquerait plus certaines métadonnées aux organismes de sécurité étrangers avec lesquels il a établi des partenariats. L'annonce faisait suite à la publication du rapport annuel 2014-2015 du Bureau du commissaire du Centre de la sécurité des télécommunications, soit l'autorité chargée de surveiller le Centre. Selon ce rapport, en raison d'une technique de filtrage devenue défaillante, de l'information révélant des détails sur les activités de communication des Canadiens n'avait pas été suffisamment minimisée (par exemple, supprimée, modifiée, cachée ou transformée autrement pour rendre impossible l'identification des personnes) avant que cette information soit communiquée aux partenaires du Groupe des cinq, plus précisément les organismes de renseignement d'origine électromagnétique de l'Australie, des États-Unis, de la Nouvelle-Zélande et du Royaume-Uni.

Comme l'indique le rapport du Bureau du commissaire du CST, le Centre a constaté à la fin de 2013 que certaines métadonnées n'avaient pas été minimisées adéquatement. Il a pu confirmer que des mesures de protection étaient en place en 2008, mais non déterminer avec certitude à quel moment le problème était survenu ou quelle quantité de métadonnées non minimisées avaient été communiquées avant 2013. Cependant, le CST nous a affirmé qu'il avait communiqué à ses partenaires de grandes quantités de métadonnées, dont certaines pouvaient avoir présenté un intérêt dans l'optique de la protection de la vie privée au Canada.

Compte tenu des répercussions possibles sur la vie privée des Canadiens, le Commissariat a examiné les circonstances à l'origine de cette situation. En avril 2016, nous avons fait part de nos observations et de nos recommandations au Centre de la sécurité des télécommunications.

ÉVALUATION, PAR LE CST, DE L'ATTEINTE À LA VIE PRIVÉE

Selon le Centre de la sécurité des télécommunications, le risque d'atteinte à la vie privée est minime pour les raisons suivantes :

- Les métadonnées ne constituaient pas des renseignements personnels sensibles puisqu'elles n'indiquaient pas le nom d'individus, ni des détails contextuels les concernant, ni la teneur des communications.

QUE SONT LES MÉTADONNÉES?

On dit habituellement que les métadonnées sont des « données sur les données ». Il s'agit de l'information concernant une communication et non du contenu d'un courriel ou d'une conversation téléphonique. Par exemple, les métadonnées d'un courriel indiqueraient le ou les destinataires; le moment où le courriel a été envoyé; l'adresse de courriel et l'adresse IP de l'expéditeur; l'adresse de courriel du destinataire; le journal des connexions du logiciel de courriel indiquant l'adresse IP; et l'objet du courriel. À l'ère numérique, nous générons constamment des métadonnées qui, une fois combinées et analysées, peuvent en dire long sur nous. Elles peuvent révéler non seulement notre identité, mais aussi nos habitudes et nos intérêts ainsi que les endroits et les personnes que nous fréquentons. Pour mieux comprendre et faire connaître les répercussions possibles sur la vie privée, le Commissariat a mené de vastes travaux de recherche sur les métadonnées.

- Il faudrait procéder à une analyse approfondie des métadonnées pour identifier des individus en particulier.

- Les partenaires du Groupe des cinq se sont tous engagés à exercer leurs activités dans le respect de la vie privée des citoyens des autres partenaires membres du Groupe.

DES GARANTIES INSUFFISANTES

Nous avons soulevé des questions concernant l'affirmation du CST selon laquelle le risque serait faible, pour les raisons suivantes :

- En ce qui concerne la sensibilité éventuelle des données communiquées aux autres partenaires du Groupe des cinq, les recherches réalisées par le Commissariat et par d'autres organisations, notamment l'Université Stanford, qui a publié récemment un rapport à ce sujet, indiquent que les métadonnées peuvent révéler des renseignements très sensibles concernant les activités, les relations, les champs d'intérêt et d'autres éléments de la vie d'un individu.

- En ce qui concerne l'engagement des partenaires du Groupe des cinq à ne pas espionner les citoyens des autres pays de ce groupe, nous n'avons aucune raison de douter de leur bonne foi, mais les assurances de ce genre ne peuvent pas être considérées comme des garanties absolues. En fait, les responsables du CST nous ont laissé entendre que les États prendraient éventuellement toutes les mesures nécessaires pour protéger leur sécurité et les intérêts nationaux.

- Le CST a reconnu avoir communiqué par inadvertance une grande quantité de métadonnées aux autres partenaires du Groupe des cinq.

À la lumière de notre examen, nous avons recommandé au CST de soumettre le programme à une EFVP complète avant de reprendre la communication des métadonnées, conformément à la directive du Secrétariat du Conseil du Trésor concernant ce type d'évaluation. Nous lui avons aussi offert de mettre l'expertise du Commissariat à son service pour l'aider à clarifier le sens de la directive ministérielle sur les métadonnées. Nous avons en outre recommandé de modifier la *Loi sur la défense nationale* non seulement pour clarifier les pouvoirs du Centre, comme l'a recommandé le Bureau du commissaire du Centre de la sécurité des télécommunications, mais aussi pour que ces pouvoirs puissent être accompagnés des garanties suffisantes pour protéger la vie privée des Canadiens.

L'accès sans mandat et la nécessité constante d'une transparence accrue

La controverse juridique entourant la question de « l'accès sans mandat » renvoie à la pratique des organismes d'application de la loi qui demandent aux fournisseurs de services de télécommunications et d'accès Internet des renseignements sur des personnes sans avoir obtenu au préalable l'autorisation d'un juge.

Dans *R. c. Spencer*, la Cour suprême du Canada a déclaré qu'il est toujours nécessaire d'obtenir un mandat sauf dans les cas où 1) il y a des circonstances contraignantes, par exemple, lorsqu'il est nécessaire d'obtenir les renseignements pour prévenir un préjudice physique imminent; 2) une loi raisonnable autorise l'accès; 3) il n'y a pas d'attente

raisonnable en matière de respect de la vie privée à l'égard des renseignements recherchés.

Depuis cet arrêt rendu en juin 2014, de nombreux fournisseurs de services de télécommunications ou d'accès Internet exigent un mandat ou une ordonnance de communication lorsque la police demande des données confidentielles sur un abonné.

Certains dirigeants d'organismes d'application de la loi se disent incapables de faire leur travail dans ces conditions. Ils soutiennent que ce type d'exigence prévu par la loi est insoutenable alors que les criminels sont de plus en plus actifs en ligne, où l'anonymat est souvent la norme.

Cependant, une adresse IP peut en révéler beaucoup sur une personne. En ayant accès aux renseignements de base concernant un abonné en lien avec ses activités sur Internet, on peut découvrir des détails sur ses intérêts d'après les sites Web consultés, les organisations dont il fait partie, les endroits où il s'est rendu et les services en ligne auxquels il s'est inscrit.

En dernière analyse, les tribunaux, en raison de leur impartialité, sont les mieux placés pour décider si des renseignements personnels sensibles doivent être communiqués aux forces policières. Il est normal et souhaitable que les tribunaux jouent le rôle d'arbitre entre les intérêts de l'État et ceux des citoyens. L'accès sans mandat devrait toujours n'être autorisé que dans des circonstances exceptionnelles.

... nous espérons qu'elles constateront les **bienfaits de la transparence** et communiqueront au public de l'information pertinente.

PROGRÈS SUR LE FRONT DE LA TRANSPARENCE

À la suite de la décision historique de la Cour suprême dans *R. c. Spencer*, certains fournisseurs de services de télécommunications et d'autres services ont commencé à présenter sur une base volontaire des rapports concernant les demandes reçues des autorités gouvernementales sollicitant des renseignements sur leurs clients. Ces rapports nous semblent utiles, mais leur forme et leur contenu varient d'un fournisseur de services à l'autre, si bien qu'il nous est difficile de connaître exactement le nombre de demandes émanant des autorités gouvernementales, les types de demandes en question et les réponses des fournisseurs.

En juin 2015, après avoir consulté le Commissariat et divers autres intervenants, Innovation, Sciences et Développement économique Canada a publié à l'intention des organisations du secteur privé de nouvelles *Lignes directrices concernant la production de rapports sur les mesures de transparence* sur lesquelles nous avons formulé des observations. La production de rapports se fait encore sur une base volontaire. Les Lignes directrices ont pour but d'accroître l'uniformité des rapports et de mieux renseigner les Canadiens sur la fréquence à laquelle les entreprises communiquent des renseignements personnels sur leurs clients aux organismes d'application de la loi et de sécurité et les situations dans lesquelles elles le font.

Pour l'avenir, nous espérons que les entreprises se conformeront aux Lignes directrices et que les rapports de transparence seront plus uniformes. En ce qui concerne les entreprises qui n'ont pas encore produit ce type de rapports, nous espérons qu'elles constateront les bienfaits de la transparence et communiqueront au public de l'information pertinente. Autrement, nous devrons peut-être revenir à la charge et réclamer des modifications législatives dans le domaine.

APPEL À L'ACTION DANS LE SECTEUR PUBLIC

Il s'agit d'une première étape importante, mais les rapports produits par le secteur privé ne constituent qu'une partie du tableau global. Le secteur public doit faire preuve de plus de transparence pour que les citoyens sachent comment mettre en lumière la mesure dans laquelle l'utilisation des pouvoirs accordés est proportionnelle aux risques connexes d'atteinte à la vie privée.

Pour poursuivre sur la lancée amorcée par le secteur privé, nous avons demandé aux institutions fédérales de produire elles aussi leurs rapports de transparence sur les demandes qu'elles adressent à des organisations du secteur privé pour obtenir des renseignements sur leurs clients. C'est d'ailleurs l'une des recommandations que nous avons formulées concernant la réforme de la *Loi sur la protection des renseignements personnels* (voir le chapitre 1).

Nous avons exhorté les institutions fédérales à tenir des registres exacts de leurs activités et à présenter des rapports sur le nombre de demandes d'accès licite qu'elles adressent aux entreprises de télécommunications ainsi que la nature et le but de ces demandes. Ainsi, les citoyens et le Parlement comprendraient mieux comment les institutions fédérales exercent les pouvoirs qui leur sont conférés en matière d'accès licite.

Conclusion

Tous les intervenants participant au débat sur la sécurité publique et le respect de la vie privée s'entendaient sur le fait que les choses ont beaucoup changé au cours des 20 dernières années. Désormais, les menaces à la sécurité nationale planent non seulement à l'étranger, mais aussi parfois en territoire canadien. De plus, nous sommes conscients des nouveaux défis que pose l'environnement en ligne pour le maintien de l'ordre.

Par ailleurs, des modifications législatives récentes ont suscité des inquiétudes parce qu'elles ouvrent la porte à une surveillance intrusive et à un profilage des Canadiens ordinaires.

Face aux menaces qui planent sur le monde aujourd'hui, les Canadiens attachent de l'importance à leur sécurité. Mais ils tiennent également à leur vie privée. Ils veulent s'assurer que les lois et les procédures en place respectent nos valeurs et ils souhaitent que les organismes chargés de l'application de la loi et de la sécurité nationale fassent leur travail dans le respect des lois.

Lorsqu'il est question de la sécurité et du respect de la vie privée, les Canadiens ne veulent pas privilégier l'une au détriment de l'autre. À juste titre, ils veulent les deux. Il est absolument essentiel de trouver le juste équilibre, car un déséquilibre dans un sens ou dans l'autre pourrait avoir de graves répercussions.

Pour atteindre un équilibre plus juste, nous avons recommandé, par exemple, de modifier le seuil de communication prévu dans la *Loi sur la communication d'information ayant trait à la sécurité du Canada* de manière à remplacer le critère de « pertinence » par celui de « nécessité ». À notre avis, les institutions des secteurs public et privé devraient produire des rapports sur la transparence et il faudrait prévoir dans la *Loi sur la défense nationale* des garanties efficaces pour protéger les renseignements personnels recueillis et utilisés par le Centre de la sécurité des télécommunications.

Chapitre 3 :

Le consentement et l'économie des renseignements personnels

Il est bien connu que les renseignements personnels ont une valeur commerciale. Avec le temps, les techniques de marketing se sont perfectionnées et les entreprises ont cessé de recueillir uniquement notre nom et notre adresse. Elles ont commencé à nous demander de plus en plus de renseignements personnels. Par exemple, sur la petite carte d'enregistrement d'un nouveau produit, on nous demande parfois de cocher une case pour indiquer notre revenu, de préciser si nous sommes propriétaire ou locataire et de mentionner comment nous avons entendu parler du produit que nous venons d'acheter.

... nous fournissons des **renseignements personnels** concernant nos intérêts, nos habitudes et notre emplacement.

De nos jours, ce type de transactions individuelles de collecte de renseignements où nous savions qui posait les questions et avions une chance raisonnable d'en comprendre les raisons – et pouvions décider de cocher les cases ou non – est chose du passé. Chaque fois que nous effectuons une recherche, naviguons ou faisons des achats sur Internet, que nous étoffons notre profil sur les réseaux sociaux ou que nous ajoutons une nouvelle application sur notre téléphone intelligent, nous fournissons des renseignements personnels concernant nos intérêts, nos habitudes et notre emplacement.

Il est de plus en plus difficile de savoir quels renseignements personnels sont recueillis et qui les recueille – et de comprendre les modèles d'affaires du 21e siècle reposant sur les renseignements personnels et les processus automatisés qui leur permettent de fonctionner.

Paradoxalement, le potentiel commercial de nos renseignements personnels augmente de façon spectaculaire, mais l'investissement nécessaire pour les recueillir, les stocker et les analyser est souvent minime. Nous vivons autant à l'ère des mégadonnées qu'à celle des données bon marché. Grâce aux progrès technologiques et au fait que les gens sont de plus en plus enclins à afficher en ligne des renseignements sur eux-mêmes, il est très facile et peu coûteux de recueillir des quantités phénoménales de renseignements personnels et de les utiliser à des fins commerciales – les robots Web utilisés par les polluposteurs pour recueillir des adresses de courriel ne sont qu'un exemple parmi tant d'autres.

Le droit de consentir

Dans cet environnement de plus en plus numérique, nous nous en remettons à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) pour protéger notre vie privée.

À bien des égards, le consentement est la pierre angulaire de cette loi. Avant de pouvoir recueillir, utiliser et communiquer en toute légitimité les renseignements personnels d'un individu dans le cadre d'activités commerciales, les organisations doivent obtenir son consentement. En l'absence de consentement, elles ne peuvent traiter les renseignements personnels que dans certaines situations limitées.

Toutefois, bien qu'elle ait été rédigée de façon à être neutre sur le plan technologique, la LPRPDE a été adoptée avant l'avènement du téléphone intelligent, de l'infonuagique, de Facebook, de l'Internet des objets et de nombreuses autres technologies de collecte de renseignements qui font maintenant partie de notre quotidien. De nos jours, nous ne savons plus vraiment qui traite nos données ni à quelles fins.

Dès lors, est-il équitable d'imposer aux consommateurs la responsabilité de comprendre ces flux de données complexes pour décider en toute connaissance de cause de donner ou non leur consentement? La technologie et les modèles d'affaires ont tellement évolué depuis la rédaction de la LPRPDE que bien des observateurs affirment maintenant que le modèle de consentement, tel qu'il a été conçu à l'origine dans le contexte des transactions commerciales individuelles, n'est plus adapté à la réalité.

Au cours des consultations que nous avons menées en vue d'établir nos priorités pour la protection de la vie privée, les intervenants ont soulevé de nombreuses questions concernant l'efficacité et la pertinence du modèle de consentement prévu dans la LPRPDE dans le contexte des mégadonnées et des multiples façons opaques dont nos renseignements peuvent être recueillis. Bon nombre étaient d'avis que les individus ont beaucoup plus de mal à exercer un contrôle et à donner un consentement éclairé parce que les politiques de confidentialité sont souvent difficiles à comprendre et trop longues, mais par ailleurs incomplètes ou inefficaces. Les Canadiens qui ont participé aux groupes de discussion mis sur pied dans le cadre de l'établissement de nos priorités nous ont dit à peu près la même chose : ils s'inquiètent de ne pouvoir exercer un contrôle suffisant sur leurs renseignements en ligne. Ils estiment qu'on ne leur indique pas à quelle utilisation servent leurs renseignements personnels et qui les utilise. Ils considèrent en outre que les politiques de confidentialité en ligne sont généralement incompréhensibles.

Le consentement au 21e siècle

En mai 2016, le Commissariat a publié un document de discussion sur le consentement et la protection de la vie privée. Il y examine le rôle des individus, des organisations, des organismes de réglementation et des législateurs et les attentes envers chacun d'eux dans l'avenir. Il examine aussi les mesures prises par d'autres pays pour faire face à la situation et décrit plusieurs solutions possibles.

Par exemple, le Commissariat propose des mesures qui renforceraient le consentement en permettant aux individus d'avoir un meilleur accès aux renseignements ou de gérer leurs préférences en ce qui a trait à différents services.

Les solutions possibles propres à remplacer le modèle de consentement reposent sur l'idée que la circulation de l'information est devenue trop complexe pour les Canadiens ordinaires

et que la solution ultime consiste à assouplir les exigences en matière de consentement dans certaines situations. Par exemple, l'Union européenne autorise le traitement des données sans le consentement de l'intéressé s'il est nécessaire à des fins légitimes et qu'il ne porte pas atteinte à ses droits.

Au Canada, la solution pourrait consister à élargir l'éventail des motifs valables pour le traitement des données en vertu de la LPRPDE afin d'y ajouter les intérêts commerciaux légitimes, soit en prévoyant un concept flexible, soit en définissant des intérêts légitimes précis dans la loi même. Nous pourrions aussi envisager d'y inscrire des « zones interdites » dans lesquelles la collecte, l'utilisation ou la communication de renseignements personnels seraient expressément interdites dans certaines situations.

Les solutions axées sur la gouvernance mettent l'accent sur le rôle que jouent les organisations. Il pourrait notamment s'agir de codes de pratiques de l'industrie, de marques de confiance garantissant la protection de la vie privée ou de la mise sur pied de comités d'éthique visant à protéger les consommateurs en conseillant les entreprises sur les utilisations appropriées des données.

Toutefois, ce type de solutions soulève des questions concernant le rôle des organismes de réglementation et la nature des pouvoirs nécessaires pour obliger efficacement les organisations à rendre des comptes. Le pouvoir de rendre des ordonnances et celui d'imposer des amendes, dont le Commissariat ne dispose pas à l'heure actuelle, sont des exemples de mesures d'application de la loi qui pourraient influer sur les pratiques des organisations et renforcer les mesures de protection de la vie privée des individus. En outre, à l'heure actuelle, le Commissariat est surtout en mode réaction. En règle générale, il examine les plaintes après une atteinte à la vie privée. Serait-il raisonnable d'accorder au Commissariat le pouvoir de vérifier la conformité aux lois sur la protection de la vie privée de façon plus proactive, avant que les problèmes surviennent? Bon nombre des solutions proposées pourraient être mises en œuvre dans le cadre législatif actuel, tandis que d'autres, comme l'élargissement des pouvoirs, nécessiteraient peut-être des modifications législatives.

La possibilité d'inscrire dans la loi des zones interdites ou de nouveaux motifs pour autoriser le traitement des données lorsque l'obtention du consentement n'est pas réaliste ou encore l'adoption de mesures de protection de la vie privée dès la conception – ce qui obligerait les entreprises à intégrer la protection de la vie privée à leurs nouveaux produits et services – figurent au nombre des autres solutions possibles qui pourraient relever des législateurs.

Nous avons invité les intéressés à nous faire part de leurs commentaires par écrit au sujet du document de discussion sur le consentement. À l'automne, nous discuterons directement avec des intervenants, soit des entreprises, des groupes de défense des droits, des universitaires, des enseignants, des spécialistes des technologies de l'information et des internautes ordinaires.

Il n'y a probablement pas de solution universelle. Toutefois, une combinaison de solutions pourrait aider les individus à mieux protéger leur vie privée, ce qui est notre principal objectif.

L'INTERNET DES OBJETS

L'Internet des objets – le nombre croissant d'objets physiques qui recueillent des données au moyen de capteurs et qui les transmettent sur des réseaux de télécommunications – présente des défis uniques en leur genre pour les cadres de protection de la vie privée reposant sur le consentement.

L'Internet des objets procure des avantages aux individus et à la société grâce à l'automatisation et à la surveillance accrue de tous les aspects de l'environnement, ce qui peut entraîner une meilleure gestion des ressources, des gains d'efficience et une utilisation plus pratique. Ses applications peuvent servir à réduire les coûts énergétiques dans une habitation en mettant en marche les appareils électriques pendant les périodes où les tarifs sont le moins élevés ou à gérer la circulation en surveillant le nombre de véhicules au moyen de capteurs intégrés dans la chaussée.

Comme en fait état le document de recherche sur l'Internet des objets publié par le Commissariat en février 2016, la collecte de renseignements par ce moyen est motivée par la volonté de comprendre les activités, les déplacements et les préférences des individus et de faire des déductions à leur sujet à partir de cette information. Pour les organisations, sa valeur réside non pas dans les revenus tirés de la vente d'appareils, mais plutôt dans les données produites et traitées grâce aux algorithmes de mégadonnées.

La plupart de ces données peuvent être sensibles ou le devenir si on les combine avec d'autres données de sources différentes. Par exemple, en combinant les données générées par une personne qui porte sur elle un téléphone intelligent et un appareil de suivi de la condition physique et qui habite dans une maison dotée d'un compteur intelligent, on peut établir un profil indiquant le lieu où elle se trouve, ses fréquentations, ses goûts et intérêts, sa fréquence cardiaque et l'activité qu'elle est susceptible de pratiquer à tout moment de la journée. Si on les combine avec d'autres données recueillies de différentes façons – par exemple, les activités sur Internet –, les renseignements deviennent encore plus sensibles et plus précieux.

La collecte de données au moyen d'appareils de l'Internet des objets est souvent imperceptible pour les personnes concernées. Il n'y a entre les consommateurs et les organisations aucune interface où la communication de données se fera de façon visible et transparente. En réalité, la collecte et la communication de données se font d'un appareil à un autre, sans intervention humaine, dans le cadre d'activités courantes. Il est donc de plus en plus difficile de transférer des renseignements pertinents sur les risques pour la vie privée afin d'aider les utilisateurs à décider en toute connaissance de cause s'ils donneront ou non leur consentement.

Principales conclusions d'enquête sur des questions relatives au consentement

L'AFFICHAGE D'UNE ADRESSE DE COURRIEL EN LIGNE NE SIGNIFIE PAS QUE L'ON CONSENT À RECEVOIR DES POURRIELS

Après le lancement du Centre de notification des pourriels du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), le Commissariat a constaté que le public avait fait parvenir des centaines de messages concernant les activités de marketing par courriel de Compu-Finder, fournisseur

de formation en entreprise établi au Québec. Cela a incité le Commissariat à mener sa toute première enquête en vertu des dispositions de la LPRPDE régissant la « collecte d'adresses » et découlant de la Loi canadienne anti-pourriel (LCAP).

Au cours de notre enquête, l'entreprise a déclaré qu'elle avait en sa possession en janvier 2014 environ 475 000 adresses de courriel, dont environ 170 000 avaient été recueillies au moyen d'un logiciel de collecte d'adresses. L'entreprise prétendait avoir cessé de recueillir des adresses de courriel au moyen d'un logiciel spécialisé avant l'entrée en vigueur de la LCAP, en juillet 2014, mais nous avons constaté qu'elle avait manifestement continué d'utiliser certaines de ces adresses à des fins de marketing.

Compu-Finder a déclaré recueillir des adresses de courriel sur les sites Web d'entreprises qui, à son avis, étaient susceptibles d'avoir un intérêt pour la formation qu'elle offrait et qui,

SUIVI DE L'ENQUÊTE SUR LE PROGRAMME DE PUBLICITÉ PERTINENTE DE BELL

En octobre 2013, le Commissariat a reçu un nombre sans précédent de plaintes à la suite du lancement du Programme de publicité pertinente de Bell. Ce programme prévoyait un suivi des activités de navigation des clients sur le Web, de l'utilisation des applications, des appels téléphoniques et de l'écoute de la télévision. Bell combinait ces renseignements avec les données démographiques recueillies dans les comptes des clients pour créer des profils détaillés afin d'aider les annonceurs tiers à présenter des publicités ciblées aux abonnés de Bell moyennant des frais.

Il incombait aux clients qui ne souhaitaient pas participer au programme de prendre des mesures pour s'en retirer. Nous avons conclu qu'il faudrait plutôt demander aux clients d'y adhérer explicitement ou, en d'autres mots, de signifier expressément leur consentement à cet égard.

À la suite de notre enquête, Bell a fait savoir qu'elle mettait fin au programme et qu'elle supprimerait tous les profils de clients existants qui y étaient associés. Elle a par la suite indiqué qu'elle prévoyait de lancer un programme similaire demandant le consentement positif (ou explicite) des clients et nous a demandé notre avis à ce sujet.

Compte tenu du nombre sans précédent de plaintes sur le programme initial et des répercussions possibles de ce type de publicité ciblée sur la vie privée de millions de personnes, nous avons jugé qu'il était dans l'intérêt des Canadiens que nous examinions le programme révisé de Bell et communiquions nos commentaires. À cette fin, le Commissariat a eu plusieurs discussions avec l'entreprise.

Sans être en mesure de dire si le nouveau programme répond ou non aux obligations prévues dans la LPRPDE, nous estimons qu'il constitue une amélioration par rapport à celui sur lequel nous avons fait enquête précédemment. En effet, Bell demande maintenant à ses clients s'ils souhaitent participer au programme et les clients doivent y adhérer explicitement. Comme nous l'avons déjà mentionné, nous estimons que la publicité comportementale en ligne est une activité légitime si elle est réalisée correctement avec le consentement éclairé des intéressés. Nous suggérons aux organisations des mesures à cet égard dans nos Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne.

en vertu des lois du Québec, étaient tenues de donner ce type de formation. Nous avons cependant constaté que, même si l'entreprise donnait la formation presque exclusivement en français dans ses installations de Montréal et de Québec, elle envoyait constamment des courriels à des destinataires se trouvant un peu partout au Canada, voire à l'étranger.

Compu-Finder nous a affirmé qu'elle pensait pouvoir recueillir sans consentement les adresses de courriel affichées sur les sites Web en vertu de l'exception prévue dans la LPRPDE à l'égard des renseignements auxquels le public a accès. Selon nous, cette exception ne s'appliquait pas. Compu-Finder utilisait les adresses pour vendre des services qui n'avaient pas toujours un lien direct avec les fins auxquelles les organisations avaient affiché sur leur site Web l'adresse de courriel de personnes. Par exemple, un professeur d'informatique a reçu un courriel faisant la promotion d'un cours destiné aux directeurs des finances.

Nous avons également constaté que certains sites Web où l'entreprise recueillait des adresses affichaient des avis non équivoques interdisant l'utilisation, à des fins de sollicitation, des adresses de courriel y figurant. Quoi qu'il en soit, l'exception s'appliquant aux renseignements auxquels le public a accès ne peut être invoquée lorsqu'une adresse a été recueillie au moyen d'un logiciel de collecte d'adresses.

De toute évidence, Compu-Finder n'était pas au courant des obligations en matière de protection de la vie privée qui lui incombent en vertu de la LPRPDE ou ne les respectait pas. L'entreprise a fini par accepter de mettre en œuvre toutes nos recommandations et de conclure un accord de conformité. C'était la première fois que nous utilisions ce nouvel outil, rendu possible grâce aux modifications apportées à la LPRPDE par la *Loi sur la protection des renseignements personnels numériques*, qui a reçu la sanction royale en juin 2015.

Les entreprises devraient lire attentivement les règlements d'application de la LPRPDE et s'assurer de bien les comprendre avant de déterminer si le public a vraiment accès à des renseignements. En avril 2015, nous avons également publié une fiche de conseils utiles et un guide qui décrivent les pratiques exemplaires en matière de marketing par courriel et les mesures à prendre pour se conformer aux nouvelles dispositions de la LPRPDE régissant la collecte d'adresses.

UN CLIENT OBTIENT UNE CARTE DE CRÉDIT SANS SON CONSENTEMENT

On nous demande de plus en plus souvent de consentir à la collecte et à l'utilisation de nos renseignements personnels en cliquant sur une icône sur un écran d'ordinateur. Or, cette pratique comporte des risques. Dans ce cas, par exemple, le plaignant a affirmé au Commissariat que, pendant qu'il faisait des achats dans un magasin de détail, un vendeur lui a demandé de s'inscrire à un programme de fidélisation. Le plaignant a déclaré qu'il avait accepté de s'inscrire à ce programme, mais qu'il avait été étonné de recevoir par la poste une carte de crédit du détaillant quelques semaines plus tard.

Le plaignant soutient que le vendeur ne l'a jamais informé qu'il demandait une carte de crédit. Il affirme même avoir demandé directement au vendeur si la demande avait quoi que ce soit à voir avec une carte de crédit et que celui-ci lui a répondu par la négative. Au cours de notre enquête, nous avons constaté que la plupart des renseignements figurant sur la demande de carte de crédit présentée au

nom du plaignant – à savoir son numéro de téléphone, son occupation, son revenu annuel et son loyer mensuel – étaient inexacts.

Le détaillant a fait valoir que le plaignant avait communiqué ses renseignements personnels en toute connaissance de cause dans le but d'obtenir une carte de crédit et qu'il avait consenti expressément à une vérification de solvabilité en cochant une case sur la tablette électronique utilisée par le vendeur pour consigner les renseignements. Le détaillant n'a toutefois pas été en mesure de prouver que le plaignant avait vu l'écran de la tablette, fourni tous les renseignements figurant dans la demande et compris que ces renseignements seraient utilisés pour vérifier sa solvabilité. Il n'a pas pu prouver non plus que c'était bel et bien le plaignant (et non le représentant du détaillant) qui avait coché la case de consentement en question.

Les organisations doivent reconnaître que leurs employés ne suivent pas toujours les procédures établies. C'est pourquoi il est important de mettre en place des mécanismes de contrôle supplémentaires, notamment pour vérifier que le consentement a bel et bien été obtenu. Notre *Trousse d'outils en matière de vie privée : Guide à l'intention des entreprises et des organisations* donne des directives précises indiquant aux organisations de conserver une preuve du consentement reçu.

Le détaillant a présenté ses excuses au plaignant, annulé la carte de crédit et demandé à l'agence d'évaluation du crédit de retirer du dossier du plaignant l'information concernant le compte et la demande de renseignements.

Conclusion

Les nouvelles technologies et les nouveaux modèles d'affaires soulèvent des questions importantes quant à la façon dont les Canadiens peuvent exercer véritablement leur droit de consentir à la collecte, à l'utilisation et à la communication de leurs renseignements personnels.

Le temps est venu de se pencher sérieusement sur la pertinence du modèle de consentement actuel sous le régime de la LPRPDE et aux mesures à prendre pour le renforcer ou l'améliorer.

En publiant un document de discussion, nous espérions lancer un remue-méninges national, voire international, réunissant des entreprises, des groupes de défense des droits, des universitaires, des enseignants, des spécialistes des technologies de l'information et des internautes ordinaires.

À terme, nous espérons pouvoir proposer des mesures concrètes et définir le rôle que doivent jouer les individus, les organisations, les organismes de réglementation et les législateurs pour véritablement aider les gens à exercer un meilleur contrôle sur leurs renseignements personnels.

Bon nombre de solutions proposées peuvent être mises en œuvre au moyen d'outils existants et dans le cadre législatif actuel au Canada, tandis que d'autres nécessiteront peut-être des modifications législatives. Il pourrait s'agir notamment d'apporter des modifications souhaitables aux pouvoirs du Commissariat, de lui donner la capacité d'être plus proactif dans son travail ou de créer des zones interdites, voire de nouveaux motifs juridiques pour traiter les renseignements lorsque l'obtention du consentement n'est pas réaliste.

Chapitre 4 :

La réputation et la protection de la vie privée

La réputation en ligne et ses répercussions éventuelles sur la vie des gens en ligne et hors ligne ont fait couler beaucoup d'encre, en particulier depuis l'avènement des médias sociaux. Les technologies d'Internet ont entraîné un changement de paradigme dans la façon dont la réputation se forge. Il faudrait une discussion sérieuse sur les recours à la disposition des personnes qui contestent les renseignements personnels affichés en ligne à leur sujet ainsi que sur le rôle connexe des entreprises, des organismes de réglementation, des législateurs et des individus.

Pour donner suite à sa priorité stratégique axée sur la réputation et la protection de la vie privée, le Commissariat met l'accent sur les risques d'atteinte à la réputation qui découlent de la grande quantité de renseignements personnels affichés en ligne. Nous examinons également les mécanismes en place et ceux que l'on pourrait mettre en place pour gérer ces risques ainsi que les options qui s'offrent pour s'assurer que les individus puissent exercer un certain contrôle sur leurs renseignements personnels.

... le Commissariat met l'accent sur les **risques d'atteinte à la réputation** qui découlent de la grande quantité de renseignements personnels affichés en ligne.

Au cours de l'établissement de nos priorités, les intervenants et la population canadienne ont indiqué être conscients des avantages personnels et professionnels dont ils bénéficient en participant au monde numérique. Par ailleurs, ils s'inquiètent de plus en plus de leur réputation en ligne. En fait, la difficulté d'exercer un contrôle sur la façon dont les renseignements personnels sont utilisés en ligne – et de les corriger ou de les supprimer – constitue l'une des préoccupations exprimées le plus souvent au cours de cette consultation.

Nous créons nous-mêmes notre réputation en ligne en affichant des profils et des photos ou en formulant des commentaires sur le contenu diffusé par les autres. Toutefois, d'autres personnes peuvent aussi façonner notre réputation. Une fois que nos renseignements personnels sont affichés en ligne, il peut être extrêmement difficile d'empêcher les autres de les utiliser dans différents contextes qui pourraient nuire à notre réputation. Et compte tenu du caractère persistant du contenu en ligne – lorsqu'une réputation est entachée, il peut s'avérer ardu de réparer les dommages.

Droit à l'oubli

Il peut être très difficile d'oublier ou de ne pas se faire constamment rappeler ce que les autres affichent à notre sujet, dans une intention malveillante ou louable, notamment par l'entremise des tribunaux ouverts, des journaux, du gouvernement

ouvert ou des archives. Le monde entier doit composer avec les répercussions du caractère persistant des renseignements personnels affichés en ligne et avec l'incidence éventuelle de cette situation sur le comportement et les rapports humains à long terme.

Le perfectionnement et l'utilisation généralisée des moteurs de recherche ont accru les risques d'atteinte à la réputation. Ainsi, des renseignements auxquels on ne pouvait autrefois avoir accès qu'à la suite de vastes recherches dans des archives peuvent maintenant être trouvés en quelques clics seulement. En mai 2014, la Cour de justice de l'Union européenne a statué que les moteurs de recherche doivent offrir à tous les Européens la possibilité de demander la suppression des résultats de recherche qui renvoient à des renseignements inexacts, inadéquats, non pertinents ou excessifs à leur sujet.

La décision a été rendue à la suite d'une affaire mettant en cause un Espagnol qui s'était opposé au fait que les résultats d'une recherche de son nom sur Google renvoyaient à des liens menant à des articles de journaux faisant état de dettes financières qu'il avait acquittées depuis longtemps. Selon lui, ces détails sur sa vie n'**étaient plus pertinents, mais** ils nuisaient néanmoins **à sa réputation.**

On parle souvent de cette décision quand il est question du **« droit à l**'oubli ». Les renseignements en cause ne sont pas vraiment supprimés – la décision ne vise que les résultats affichés par les moteurs de recherche. Néanmoins, la décision accorde aux individus un certain contrôle sur l'accès à leurs renseignements personnels en les rendant plus difficiles à trouver.

Lancement d'une discussion

En janvier 2016, le Commissariat a publié un document de travail portant sur la question de la réputation en ligne dans le contexte canadien et expliquant les difficultés auxquelles font face les individus en ligne lorsqu'il s'agit de protéger leur vie privée. Nous espérions ainsi stimuler la discussion sur l'ampleur de ces nouvelles difficultés et les solutions possibles.

En publiant le document de travail, notre but était d'attirer l'attention sur ce nouveau défi dans le domaine de la protection de la vie privée en vue de susciter une discussion sur les solutions. À terme, nous entendons définir la position du Commissariat relativement aux recours. Pour ce faire, nous avons invité les individus, les organisations, les universitaires, les groupes de défense des droits, les spécialistes des technologies de l'information, les enseignants et les autres parties intéressées à proposer des façons nouvelles et novatrices de protéger la vie privée et la réputation.

Plus particulièrement, nous avons mis en évidence des écarts possibles dans les mesures de protection entre le monde virtuel et le monde réel et demandé aux participants d'exprimer leur opinion à ce sujet. Nous avons aussi sollicité des idées sur des pistes de solutions pratiques, techniques, stratégiques ou législatives qu'il faudrait envisager pour atténuer les risques d'atteinte à la réputation en ligne.

Le Commissariat a reçu 26 mémoires. La consultation avait pour but d'enrichir le débat public et de faire en sorte que le Commissariat soit bien placé pour renseigner le Parlement sur les questions ayant trait à la réputation en ligne et élaborer une position de principe à ce sujet.

En plus de publier le document de travail en janvier, le Commissariat s'est penché sur la question de la réputation et de la vie privée dans les secteurs public et privé ainsi que dans l'appareil judiciaire, comme l'indiquent les exemples qui suivent.

Ashley Madison : une atteinte à la sécurité de détails intimes sur la vie privée

Dans l'économie en ligne d'aujourd'hui, des sites Web commerciaux de tous genres et de toutes tailles peuvent contenir de vastes quantités de renseignements personnels qui vont au-delà des données de paiement. En vertu de la LPRPDE, les organisations doivent tenir compte des répercussions sur la réputation des individus au moment de déterminer les mesures de protection qu'elles doivent adopter ainsi que d'autres exigences, comme celles se rapportant au consentement.

Au cours de l'été 2015, des pirates informatiques ont porté atteinte à la sécurité des serveurs de l'entreprise canadienne Avid Life Media (ALM – récemment renommée « Ruby Corp. »), qui exploite le site Web Ashley Madison s'adressant aux personnes à la recherche d'une aventure en toute confidentialité. Ils ont par la suite publié des renseignements se trouvant dans le compte d'environ 36 millions d'utilisateurs au Canada et ailleurs dans le monde.

Comme l'incident touchait des utilisateurs répartis dans une cinquantaine de pays, nous avons mené une enquête conjointe avec le Commissariat à l'information de l'Australie dans le cadre de l'Accord de coopération du Forum de coopération économique Asie-Pacifique sur la protection transfrontière des données.

L'enquête a révélé de nombreuses infractions à la LPRPDE et à la loi sur la protection des renseignements personnels de l'Australie. Elle a également donné lieu à des conclusions comportant des leçons importantes pour d'autres organisations qui détiennent des renseignements personnels :

SÉCURITÉ

Les mesures de protection mises en œuvre par ALM pour protéger les renseignements personnels n'étaient pas adéquates. Compte tenu de la sensibilité des renseignements qu'elle détenait, il était inacceptable que l'entreprise ne se soit pas dotée d'un plan de sécurité de l'information détaillé. Plus précisément, plusieurs éléments clés étaient absents du cadre de sécurité de l'entreprise, par exemple des politiques ou des pratiques en matière de sécurité de l'information bien documentées, sur lesquelles reposerait la promotion d'une culture de sensibilisation à la sécurité et de protection des renseignements personnels; un processus de gestion des risques explicite, notamment des évaluations périodiques et proactives des menaces pour la vie privée ainsi que des évaluations des pratiques de sécurité; une formation adéquate pour s'assurer que tous les membres du personnel comprennent les obligations leur incombant en matière de sécurité et de protection de la vie privée et qu'ils s'en acquittent comme il se doit.

En outre, les points faibles particuliers comme l'authentification à un seul facteur et les piètres pratiques de gestion des clés et des mots de passe constituent aussi individuellement et collectivement un défaut de prendre des mesures de protection appropriées pour protéger les renseignements personnels détenus par ALM.

CONSENTEMENT ET TRANSPARENCE

ALM n'a pas obtenu un consentement valide des utilisateurs pour recueillir leurs renseignements personnels, en ce sens qu'elle ne leur a pas expliqué clairement dès le départ ses pratiques de traitement des renseignements personnels et qu'elle a obtenu leur consentement par un subterfuge, du moins en partie. En effet, l'entreprise affichait sur sa page d'accueil une marque de confiance factice laissant entendre aux utilisateurs potentiels que ses pratiques de sécurité avaient fait l'objet d'un examen et avaient été jugées de qualité par un tiers indépendant.

CONSERVATION

ALM conservait indéfiniment les renseignements personnels des utilisateurs à moins que ceux-ci n'acquittent les frais imposés pour les faire supprimer définitivement. Or, cette pratique contrevient aux dispositions de la LPRPDE régissant la conservation, selon lesquelles les renseignements personnels ne doivent être conservés qu'aussi longtemps que nécessaire pour la réalisation des fins auxquelles ils ont été recueillis.

EXACTITUDE DES ADRESSES DE COURRIEL

En raison de la pratique selon laquelle ALM obligeait les personnes qui s'inscrivaient à fournir une adresse de courriel, sans toutefois s'assurer elle-même adéquatement de son exactitude, l'adresse de courriel de personnes ne s'étant jamais inscrites à AshleyMadison a été affichée en ligne à la suite de l'incident. On sait que cette pratique a créé des risques d'atteinte à la réputation de non-utilisateurs et qu'elle contrevenait aux exigences d'exactitude imposées par la LPRPDE.

Dans la foulée de notre enquête conjointe, ALM a accepté de prendre des mesures pour donner suite aux préoccupations énoncées ci-dessus. Nous en sommes heureux mais nous ferons un suivi pour vérifier que l'entreprise a respecté les engagements qu'elle a pris en vertu d'un accord de conformité conclu avec elle au terme de l'enquête.

En plus de montrer à quel point il est important de prendre en compte les risques d'atteinte à la réputation au moment de s'assurer que des mesures de protection appropriées sont en place, cet incident fait la preuve qu'il faut accorder un soin particulier à la formulation des énoncés en matière de sécurité et de confidentialité à l'intention des consommateurs pour leur permettre de donner un consentement éclairé.

Comme le montre aussi cette affaire, malgré la diminution constante des coûts de stockage des données, la conservation de renseignements personnels alors qu'ils ne sont plus nécessaires pour la réalisation des fins auxquelles ils ont été recueillis comporte des coûts réels et un risque d'atteinte à la vie privée pour les individus et les organisations.

Les lacunes observées dans cette affaire ne sont malheureusement pas exceptionnelles. Toutes les entreprises qui gèrent de grandes quantités de renseignements personnels – et elles sont nombreuses en 2016 – peuvent en tirer des leçons.

Globe24h.com : un risque mondial d'atteinte à la réputation

Une fois que nos renseignements personnels sont affichés en ligne, il peut être très difficile de contrôler leur diffusion et leur utilisation, même si les mesures de protection et les intentions sont les meilleures qui soient. Contrairement à Internet, les mesures de protection de la vie privée ne transcendent pas toujours facilement les frontières internationales. De toute évidence, une coopération à l'échelle mondiale s'impose pour protéger la réputation des individus, comme en témoigne l'affaire Web Globe24h.com, site Web exploité en Roumanie qui republie des décisions judiciaires, y compris celles de tribunaux canadiens.

Conscients que ces décisions peuvent contenir des renseignements personnels sensibles, les tribunaux canadiens n'autorisent pas l'indexation des documents selon le nom des personnes en cause. Par conséquent, si un utilisateur entre le nom d'une personne dans un moteur de recherche, il n'obtiendra pas de liens menant à des décisions judiciaires où figure ce nom.

Le site Globe24h.com prive les individus de cette protection lorsqu'il republie les documents et permet par le fait même d'effectuer une recherche par nom. Le Commissariat a reçu plus d'une vingtaine de plaintes concernant le site en question. Par exemple, une plainte a été déposée au nom de la fille d'une plaignante qui était nommément désignée et décrite comme « travailleuse du sexe » dans une affaire où elle avait comparu à titre de témoin. Ce document de la cour était le premier résultat affiché lorsque l'on faisait une recherche en ligne en utilisant le nom de cette personne.

Comme l'indiquait notre rapport annuel de 2014 concernant la LPRPDE, notre enquête a révélé que Globe24h.com offrait aux personnes visées la possibilité de faire supprimer leurs renseignements personnels du site moyennant un paiement – pouvant atteindre des centaines de dollars. À notre avis, dans les circonstances, une personne raisonnable ne jugerait pas qu'il s'agit d'un modèle d'affaires approprié. Qui plus est, nous avons aussi constaté que le site Web n'obtenait pas un consentement valable des personnes concernées.

De surcroît, le site Web soutient qu'il n'est pas assujetti à la loi canadienne et rejette donc notre demande de retirer de ses serveurs et des mémoires caches des moteurs de recherche les décisions des tribunaux canadiens.

Soucieux de faire appliquer nos recommandations, un des plaignants initiaux a intenté une poursuite contre le site Web devant la Cour fédérale du Canada. Le Commissariat a obtenu le statut de partie intéressée dans cette affaire, qui soulève plusieurs questions, dont la mesure dans laquelle la LPRPDE s'applique à un site Web établi à l'étranger.

Entre-temps, le Commissariat a réussi à convaincre les représentants de certains moteurs de recherche importants de retirer de leur plein gré les liens menant au site Web de Globe24h ou d'en réduire l'importance dans les résultats de recherche.

Conclusion

D'énormes changements technologiques survenus sur une période relativement courte ont créé de nouveaux défis pour les individus ainsi que pour les cadres réglementaire, législatif et juridique. Même en faisant preuve d'une grande prudence à l'égard du contenu les concernant qu'ils affichent en ligne, les individus exercent peu de contrôle sur ce que d'autres personnes peuvent afficher à leur sujet ou sur la façon dont leurs activités en ligne – de leurs achats à leurs lectures – peuvent être interprétées par divers algorithmes.

Des questions juridiques importantes demeurent sans réponse. Il faudra d'abord examiner l'efficacité des mesures actuelles de protection de la vie privée. La LPRPDE est maintenant en vigueur depuis plus de 15 ans, et bon nombre des risques d'atteinte à la réputation en ligne observés aujourd'hui n'existaient pas au moment de sa promulgation. Nous devons nous demander comment certains de ses principes de base – assurer l'exactitude des renseignements personnels détenus par les organisations; limiter la collecte, l'utilisation et la communication des renseignements à ceux qui sont nécessaires pour réaliser les fins déterminées; et veiller à ce que les individus aient véritablement la possibilité de retirer leur consentement – peuvent être appliqués efficacement dans un monde de plus en plus caractérisé par l'analyse automatisée des données en ligne persistantes.

Chapitre 5 :

Le corps comme source d'information

L'essor des technologies numériques dans le domaine de la santé ou la collecte, l'utilisation et la communication de données biométriques à des fins commerciales, récréatives et judiciaires se traduisent par une utilisation accrue de nos renseignements les plus personnels, c'est-à-dire ceux se rapportant à notre corps.

Toute une industrie mondiale exploitant l'information sur le corps humain, par exemple les résultats d'analyses sanguines ou de tests génétiques, a vu le jour. De plus en plus d'appareils utilisés pour recueillir ces renseignements – appareils de suivi de la condition physique, pèse-personnes, etc. – sont connectés à l'Internet des objets et permettent ainsi de recueillir, d'analyser et de communiquer des quantités sans précédent de nos renseignements personnels les plus intimes.

Le mode d'utilisation ou de communication de ces renseignements pourrait avoir une incidence sur de nombreuses facettes de notre vie, par exemple notre assurabilité ou notre employabilité future ou nos relations personnelles. Dans le cas des tests génétiques, notre famille pourrait aussi être touchée.

En résumé, la technologie a transformé le **risque d'atteinte** à la sécurité de nos renseignements personnels les plus intimes.

En résumé, la technologie a transformé le risque d'atteinte à la sécurité de nos renseignements personnels les plus intimes. Or, les outils et les connaissances générales qui pourraient permettre aux individus d'exercer un contrôle sur ces renseignements très personnels n'ont pas évolué au même rythme.

Avantages possibles, risques et préoccupations véritables

Au cours de l'établissement de nos priorités, les intervenants et les participants aux groupes de discussion ont convenu que les renseignements se rapportant au corps nécessitent une attention particulière en raison de leur sensibilité.

Devant l'émergence des technologies et des pratiques nouvelles concernant le corps humain, les participants ont reconnu les nombreux avantages que peuvent procurer à la société les progrès réalisés dans les domaines de biomédical et d'autres progrès technologiques qui touchent le corps. Parallèlement, ils ont souligné l'importance d'assurer l'anonymat de ces renseignements et d'adopter une approche proactive afin de cerner leurs répercussions sur la vie privée et de les atténuer. De nombreux intervenants ont exprimé des préoccupations particulières concernant l'application de l'analyse des mégadonnées aux renseignements sur la santé et aux renseignements génétiques et

biométriques. Ils ont souligné les risques liés aux utilisations secondaires préjudiciables, qu'il s'agisse de marketing, d'assurance ou d'utilisations futures que nous ne pouvons même pas encore imaginer. Selon certains, des restrictions claires s'imposent dans le domaine.

D'autres estiment qu'il faut accroître la transparence pour permettre aux individus de mieux savoir quels renseignements sont recueillis, par qui et à quelles fins. D'autres encore sont d'avis que les renseignements personnels des membres des groupes vulnérables, par exemple ceux qui dépendent d'appareils médicaux, sont le plus à risque. La sécurité constitue par ailleurs une préoccupation importante compte tenu de la sensibilité des renseignements, de leur attrait pour les criminels et de leur vulnérabilité au piratage.

La plupart des Canadiens sont préoccupés par ces enjeux. Par exemple, dans notre sondage de 2014 auprès des Canadiens sur la protection de la vie privée, plus de 80 % des répondants se sont dits préoccupés par l'utilisation des résultats de tests génétiques à des fins non reliées à la santé et 70 % se sont dits préoccupés dans une certaine mesure par l'utilisation d'accessoires intelligents qui recueillent des renseignements personnels sur ceux qui les portent sur eux.

Compréhension des enjeux

Les accessoires intelligents à porter sur soi et les autres appareils branchés à Internet, comme les pèse-personnes intelligents, les dispositifs de surveillance du sommeil et les autres produits liés à la santé, peuvent non seulement recueillir, mais aussi communiquer certaines de nos données les plus intimes. Par exemple, les appareils de suivi de la condition physique connectés avec le téléphone intelligent de l'utilisateur peuvent ensuite établir une liaison avec une application infonuagique qui évalue les données de l'intéressé, lui donne des conseils et lui permet de communiquer les résultats aux membres de son réseau.

Compte tenu de la sensibilité de l'information, il est essentiel que les entreprises offrant ces appareils fassent preuve de transparence quant aux renseignements recueillis, à la façon dont ils seront utilisés et à qui ils seront communiqués. Conformément à sa priorité stratégique axée sur le corps comme source d'information – dont l'objectif est de promouvoir le respect de la vie privée et de l'intégrité du corps humain comme véhicule de nos renseignements personnels les plus intimes –, le Commissariat compte soumettre à une analyse de contexte les nouvelles applications et technologies numériques dans le domaine de la santé qui sont offertes sur le marché et d'examiner leurs répercussions sur la vie privée.

À la lumière des résultats de l'analyse de contexte, du ratissage pour la protection de la vie privée du Global Privacy Enforcement Network (GPEN) et d'autres recherches en laboratoire, le Commissariat prévoit d'élaborer des orientations à l'intention des concepteurs de ces appareils et des applications connexes – tout particulièrement les petites et moyennes entreprises et les développeurs d'applications – sur la façon d'intégrer des mécanismes de protection de la vie privée dans leurs nouveaux produits et services. Ces travaux aideront à éclairer nos efforts d'éducation et de sensibilisation pour faire connaître aux Canadiens les risques d'atteinte à la vie privée associés aux accessoires intelligents à porter sur soi.

Ratissage international pour la protection de la vie privée : le Commissariat met l'accent sur les technologies dans le domaine de la santé

On estime que le nombre d'accessoires intelligents à porter sur soi pour le sport et d'accessoires sans fil pour le suivi de la santé atteindra 170 millions d'ici 2017. La prolifération de ces appareils et les préoccupations qu'elle soulève sur le plan de la protection de la vie privée ont incité le GPEN à consacrer à l'Internet des objets le ratissage international pour la protection de la vie privée qui s'est déroulé en avril 2016. Le thème de cette année concorde avec d'autres initiatives menées par le Commissariat dans ce domaine en émergence.

Le ratissage a mis à contribution des autorités de protection des données de partout dans le monde, y compris le Commissariat, ainsi que les organismes analogues de l'Alberta, de la Colombie-Britannique, de la Nouvelle-Écosse et de l'Ontario. Dans le cadre de l'initiative de cette année, les autorités ont accordé une attention particulière à la responsabilité et ont examiné les communications concernant la protection des renseignements personnels se rapportant aux appareils connectés à Internet ainsi que les pratiques dans le domaine.

Chaque autorité participante a pu choisir une catégorie de produits différente et adopter l'approche qui lui convenait. Ainsi, certaines se sont penchées sur les accessoires intelligents à porter sur soi ou les appareils électroménagers, tandis que d'autres ont examiné des objets bien précis, comme les compteurs intelligents, les voitures connectées ou les télévisions intelligentes. Le Commissariat s'est concentré sur les appareils médicaux en renforçant et en complétant ainsi d'autres initiatives en cours ou prévues qui sont en lien avec sa priorité stratégique du corps comme source d'information et en aidant à promouvoir la conformité parmi les concepteurs et à sensibiliser les utilisateurs de ces appareils à la protection de la vie privée.

En plus de mettre l'accent sur différents types d'appareils, les autorités de protection des données et de la vie privée participant au ratissage l'ont abordé sous différents angles. Certaines ont acheté des produits et évalué les communications concernant la protection de la vie privée auxquelles le consommateur a accès au moment de l'achat. Elles ont même utilisé les produits pour constater par elles-mêmes la nature des renseignements personnels recueillis et savoir s'ils concordaient avec les affirmations des fabricants ou des détaillants à ce sujet. D'autres ont plutôt examiné l'information sur la protection de la vie privée qui est affichée sur le site Web du fabricant. Dans certains cas, les autorités ont pu communiquer directement avec le fabricant, le détaillant ou le responsable du traitement des données pour lui poser des questions précises concernant la protection de la vie privée. Le Commissariat a utilisé ces trois méthodes dans le cadre de son examen des appareils médicaux.

Le ratissage visait à sensibiliser davantage le public et les entreprises aux droits et aux responsabilités en matière de protection de la vie privée, à encourager la conformité aux lois qui assurent cette protection, à déterminer les préoccupations auxquelles on peut répondre en prenant des mesures ciblées de sensibilisation ou d'application de la loi et à renforcer la coopération entre les autorités chargées de l'application des lois sur la protection de la vie privée.

Au moment de la rédaction du présent rapport, les responsables compilaient les résultats du ratissage en vue de leur publication à l'automne 2016. Comme par les années passées, les préoccupations soulevées pendant le ratissage pourraient donner lieu à des activités de suivi, par exemple la sensibilisation d'organisations ou l'adoption de mesures d'application de la loi.

Dialogue sur la génétique à l'échelle nationale et internationale

Partout dans le monde, les autorités de protection des données et de la vie privée sont aux prises avec ces enjeux et d'autres risques d'atteinte à la vie privée associés aux tests génétiques. Par exemple, en octobre 2015, les participants à la Conférence internationale des commissaires à la protection des données et de la vie privée – dont le Commissariat – se sont penchés sur les défis découlant de la capacité croissante de la société à recueillir, à analyser et à utiliser des renseignements génétiques.

Comme l'ont reconnu les participants à la conférence, même s'il est manifeste que l'accès aux renseignements génétiques présente et continuera de présenter de nombreux avantages, leur collecte et leur utilisation pourraient comporter divers risques, notamment ceux de discrimination ou de refus de services en raison des prédispositions génétiques. À l'issue de la conférence, ils ont réclamé l'adoption de mesures rigoureuses de protection de la vie privée en déclarant qu'il était essentiel que les individus puissent continuer d'exercer un contrôle sur leurs données, recevoir de l'information appropriée sur les options à leur disposition et s'assurer que leurs choix sont respectés. Selon eux, ces éléments sont particulièrement importants dans le cas des résultats de tests génétiques, qui peuvent révéler des renseignements très sensibles sur les individus et leur famille.

En juin 2015, l'Association francophone des autorités de protection des données personnelles, dont fait partie le Commissariat, a elle aussi réclamé l'adoption de nouvelles mesures de protection pour faire face à ces enjeux. Elle a également adopté une résolution sur le traitement des données à caractère personnel dans le domaine de la santé et de la génétique.

En participant à ce type de tribunes internationales et en menant ses travaux de recherche, ses activités parlementaires et d'autres activités de sensibilisation, le Commissariat continue de cerner les risques actuels et éventuels sur le plan de la protection de la vie privée associés aux tests génétiques et à attirer l'attention sur ceux-ci. Il poursuit aussi sa collaboration avec des organismes analogues au Canada et à l'étranger afin de proposer des façons d'atténuer ces risques, dont aucun n'était prévu au moment de la rédaction des lois actuelles sur la protection de la vie privée. Au cours du prochain exercice, le Commissariat publiera de concert avec des commissariats provinciaux une fiche d'information sur les services de dépistage génétique offerts directement aux consommateurs. Il souhaite ainsi renseigner les individus sur les risques d'atteinte à leur vie privée et leur donner des orientations sur les options leur permettant de se protéger.

En 2015-2016, le Commissariat a continué de participer en tant que membre d'office du Comité consultatif de la banque nationale de données génétiques. Ce comité s'est alors concentré sur la mise en œuvre prévue de nouveaux indices se rapportant au profil génétique de restes humains, de victimes,

de bénévoles ainsi que de personnes portées disparues et de leurs proches.

Projet de loi sur la discrimination génétique

En février, le commissaire a témoigné devant le Comité sénatorial permanent des droits de la personne dans le cadre de l'examen du projet de loi S-201, *Loi visant à interdire et à prévenir la discrimination génétique*.

Le projet de loi interdirait globalement la pratique consistant à exiger la collecte des résultats de tests génétiques pour fournir des biens ou des services – comme une police d'assurance – ou conclure un contrat et il exigerait le consentement écrit des personnes qui choisissent de communiquer ces renseignements.

À la suite de la présentation du mémoire du commissaire, le projet de loi S-201 a été modifié pour tenir compte de notre recommandation, selon laquelle le consentement écrit d'un individu devrait également être requis pour communiquer les résultats de tests génétiques à quelque fin que ce soit. Le Comité a aussi accepté notre recommandation de ne pas ajouter explicitement les renseignements tirés de tests génétiques à la définition de « renseignements personnels » énoncée dans la *Loi sur la protection des renseignements personnels* et la LPRPDE étant donné que ces renseignements sont déjà visés par ces lois.

Le projet de loi a été adopté par le Sénat le 14 avril 2016 et il a été renvoyé à la Chambre des communes, où il sera débattu.

Conclusion

Ce ne sont là que quelques-uns des nombreux défis qu'il faudra relever pour protéger la vie privée ainsi que l'intégrité du corps et de l'esprit contre les risques croissants liés aux technologies en constante évolution – comme les accessoires intelligents à porter sur soi, la biométrie, la génomique, la robotique et l'intelligence artificielle – qui permettent de recueillir et d'utiliser des renseignements personnels par des moyens nouveaux et subtils.

Comme pour les enjeux concernant le consentement traités au chapitre 3, dans ce contexte en évolution rapide, nous devons trouver des réponses aux questions découlant de cette nouvelle réalité et déterminer quels sont les nouveaux outils nécessaires et comment améliorer ceux qui existent déjà pour aider les individus à bénéficier des avantages des nouvelles technologies prometteuses tout en gérant efficacement les risques d'atteinte à leur vie privée.

Chapitre 6 :

Rétrospective de l'exercice

Au cours de l'exercice, le Commissariat a poursuivi toute une gamme d'autres activités visant à protéger et à promouvoir le droit des individus à la vie privée.

Les activités présentées dans les chapitres précédents font ressortir les enjeux et les efforts se rapportant directement à nos quatre priorités stratégiques liées à la vie privée ainsi que la nécessité d'adapter la *Loi sur la protection des renseignements personnels* aux réalités du 21e siècle. Mais le Commissariat a mené beaucoup d'autres travaux importants tout au long de l'exercice. Le présent chapitre résume ces autres activités clés et cite quelques exemples.

Éducation et sensibilisation du public

Il est essentiel d'améliorer la sensibilisation du public afin d'informer les organisations de leurs obligations en matière de protection de la vie privée, de renseigner les individus sur les mesures à prendre pour protéger leur droit à la vie privée et de maintenir la confiance à l'égard de l'économie numérique.

Au cours de l'exercice écoulé, nous avons renforcé certaines activités de sensibilisation en utilisant les ressources à notre disposition. Nous avons notamment élaboré des stratégies ciblant les jeunes, les aînés et les petites entreprises, car nous avons déterminé au cours de l'établissement de nos priorités qu'il serait profitable pour ces groupes de recevoir plus d'information sur les questions liées à la protection de la vie privée.

Nos efforts de conscientisation reposant sur la communication, l'éducation du public et la sensibilisation passent par une large gamme d'activités – réunions avec des intervenants, allocutions, kiosques dans des expositions, élaboration et distribution de matériel de référence, souvent par l'entremise de notre site Web, etc.

Par exemple, en 2015-2016 :

- Nous avons donné plus d'une centaine d'allocutions et de présentations d'un bout à l'autre du pays devant des publics et des intervenants très variés – Conférence sur l'accès à l'information et la protection des renseignements personnels tenue à l'Université de l'Alberta, congrès Countermeasure 2015 réunissant les professionnels de la sécurité des technologies de l'information (TI), Sommet sur les jeunes et le numérique, etc.

- Nous avons tenu un kiosque lors d'une quarantaine d'autres événements afin de joindre les groupes ciblés dans le cadre de l'établissement de nos priorités et de mobiliser les intervenants.

- Notre bureau de Toronto – une présence régionale qui tire sa raison d'être du grand nombre d'entreprises assujetties à la LPRPDE ayant leur siège social dans cette ville – a continué de jouer un rôle clé dans les relations avec les intervenants et les activités de sensibilisation. Depuis janvier 2015, l'équipe a mené 128 activités de sensibilisation et de relations avec les intervenants et élaboré de nouveaux produits d'information, par exemple les fiches d'information intitulées *Dix trucs pour empêcher les employés de fureter* et *Collecte auprès des enfants? Dix conseils sur les services destinés aux enfants et aux jeunes*.

Par ailleurs, le Commissariat a apporté d'importantes améliorations au contenu et à la convivialité de son site Web afin que les Canadiens et les organisations puissent avoir accès à de l'information claire, compréhensible et pertinente sur les questions liées à la protection de la vie privée. En effet, les individus et les entreprises nous ont dit se tourner d'abord vers Internet lorsqu'ils ont besoin d'aide sur des questions relatives à la vie privée. L'amélioration continue du site Web du Commissariat demeurera donc une priorité.

En plus de consulter le site Web du Commissariat, les Canadiens et les organisations nous font parvenir environ 9 000 demandes par an pour obtenir des conseils. En 2015-2016, nous avons créé deux nouveaux outils afin d'aider les individus à contacter le Commissariat pour soulever des questions et lui faire part de préoccupations concernant la protection de la vie privée, soit un formulaire en ligne « intelligent » à l'intention de ceux qui préfèrent poser leurs questions par voie électronique et un nouveau formulaire de commentaires qui permet aux personnes d'exprimer leurs préoccupations sur les questions liées à la vie privée pour nous aider à établir des tendances et à étayer d'éventuelles mesures.

Comme nous l'avons déjà mentionné, le Commissariat a aussi commencé à mettre en œuvre des stratégies pluriannuelles de communication et de sensibilisation afin de mieux atteindre et sensibiliser les trois principaux groupes cibles.

SENSIBILISATION DES PETITES ENTREPRISES

En règle générale, plus une entreprise est petite et moins il est probable qu'elle dispose de ressources à l'interne pour la conseiller sur la protection de la vie privée. C'est pourquoi le Commissariat cible les plus petites entreprises du pays afin de les sensibiliser à leurs obligations dans le domaine et de leur fournir des orientations et de l'information sur le sujet.

Pour mieux comprendre les besoins en information des petites entreprises, le Commissariat a formé des groupes de discussion composés de propriétaires et d'employés de petites entreprises dans trois villes canadiennes. Il a par la suite peaufiné ses activités de sensibilisation en tenant compte des idées recueillies dans le cadre de ces discussions.

Des membres du personnel du Commissariat ont discuté avec divers groupes du milieu des petites entreprises, entrant ainsi en contact avec environ 14 000 personnes au cours de l'exercice. Ils ont notamment participé à de nombreux événements organisés avec les

chambres de commerce locales dans différentes villes partout au pays.

Outre ces vastes initiatives, notre stratégie axée sur les petites entreprises fait appel à une approche sectorielle qui cible les secteurs à l'origine du plus grand nombre d'appels et de plaintes adressés au Commissariat. Par exemple, nous nous sommes efforcés de nouer des liens avec des associations clés dans les secteurs de l'hébergement et du commerce de détail et d'explorer les possibilités de collaborer avec elles.

SENSIBILISATION DES JEUNES

Entre autres activités de sensibilisation des jeunes, nous avons élaboré un outil interactif en ligne intitulé « Règles à la maison » pour aider les parents à en apprendre davantage sur les activités en ligne de leurs enfants et à discuter avec eux des moyens de protéger leur vie privée sur Internet.

Nous avons aussi créé une activité en classe s'inspirant des ratissages dont il a été question dans le présent rapport. Nous avons transmis le matériel de cette activité aux écoles d'un bout à l'autre du pays afin d'aider les enseignants à faire connaître aux élèves les politiques de confidentialité et les enjeux liés à la protection de la vie privée en lien avec la collecte de renseignements personnels en ligne.

Ratissage international pour la protection de la vie privée – pleins feux sur les jeunes

Le Commissariat s'est joint à des autorités de protection des données d'une vingtaine de pays afin de mener à bien le troisième ratissage annuel du Global Privacy Enforcement Network (GPEN) pour la protection de la vie privée en mai 2015. Ce ratissage portait sur les applications et les sites Web ciblant les enfants ou populaires auprès d'eux.

Malgré quelques exemples novateurs de mesures de contrôle, comme l'utilisation d'un nom d'utilisateur prédéfinis et d'un avatar pour éviter que les enfants se servent de leur nom véritable ou d'une photo personnelle, nous avons constaté que trop de concepteurs recueillent des renseignements personnels particulièrement sensibles auprès des enfants – photos, vidéos et emplacement – et permettent souvent que ces renseignements soient affichés ou partagés avec des tiers. Cette pratique soulève de sérieuses questions sur les possibilités d'atteinte à la réputation et au bien-être.

On peut trouver plusieurs exemples précis à ce sujet dans un billet de blogue affiché sur le site Web du Commissariat. L'équipe de ratissage du Commissariat, qui comprenait plusieurs enfants, a examiné 172 sites Web et applications. Les jeunes membres de l'équipe, qui étaient accompagnés de leurs parents, ont formulé leurs observations dans un billet de blogue distinct.

SENSIBILISATION DES AÎNÉS

Notre stratégie de sensibilisation des aînés met l'accent sur l'élaboration et la communication d'information et d'orientations. Elle vise à répondre aux préoccupations particulières de ce groupe, comme le vol d'identité, l'hameçonnage et les autres arnaques en ligne, ainsi qu'aux questions liées à la protection de la vie privée en lien avec les réseaux sociaux et l'utilisation d'appareils mobiles.

Au cours de l'exercice écoulé, le Commissariat a mené deux campagnes à la radio sur la protection de la vie privée et le vol d'identité, distribué le document intitulé *Le vol d'identité et vous* dans les bibliothèques de tout le pays et donné des présentations dans le cadre de nombreux événements s'adressant aux aînés. Il a ainsi sensibilisé quelque 45 000 personnes dans diverses villes et poursuivra ses efforts de sensibilisation auprès des membres de ce groupe vulnérable important.

Activités parlementaires

Au cours de l'exercice, le Commissariat a formulé des commentaires sur de nombreuses mesures législatives proposées et sur d'autres questions susceptibles d'avoir des répercussions sur la vie privée. Nous avons exprimé notre opinion à 20 reprises en présentant des mémoires à des comités de la Chambre des communes et du Sénat ou en témoignant devant eux. Le Commissariat a ainsi formulé ses observations sur les projets de loi C-51 et S-201 et sur la réforme de la *Loi sur la protection des renseignements personnels*, dont il est question dans d'autres chapitres du rapport, de même que sur les projets de loi suivants :

Projet de loi C-26, Loi sur le renforcement des peines pour les prédateurs d'enfants

Dans son témoignage devant le Comité sénatorial permanent sur les affaires juridiques et constitutionnelles, en juin 2015, le Commissariat s'est concentré expressément sur l'efficacité générale de la *Loi sur l'enregistrement de renseignements sur les délinquants sexuels* (LERDS) et sur l'intérêt de créer une banque de données accessible au public sur les délinquants sexuels à risque élevé. Après avoir été adopté sans amendement, le projet de loi a reçu la sanction royale le 18 juin 2015.

Projet de loi C-377, Loi modifiant la Loi de l'impôt sur le revenu

En vertu de ce projet de loi, les syndicats seraient tenus de communiquer leurs paiements, le nom et le salaire de leurs employés ainsi que leurs activités politiques sur un site Web de l'Agence du revenu du Canada. Le Commissariat a soulevé plusieurs préoccupations au cours de son témoignage devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles en mai 2015. Entre autres, une disposition visant à associer publiquement le nom de certaines personnes à leurs activités politiques nous semblait particulièrement troublante du point de vue de la protection de la vie privée. Le projet de loi a été adopté, mais au moment de la rédaction du présent rapport, il faisait l'objet d'une mesure d'annulation par l'actuel Parlement.

Projet de loi C-59, Loi nº 1 sur le Plan d'action économique de 2015

En juin 2015, à l'invitation du Comité sénatorial permanent des finances nationales, le Commissariat a exprimé son point de vue

sur certaines parties du projet de loi C-59 ayant de nombreuses répercussions sur la vie privée. Il s'agit notamment des dispositions autorisant le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) à communiquer des renseignements, à des fins d'enquête, aux organismes provinciaux chargés d'administrer la législation sur les valeurs mobilières et étendant la collecte de données biométriques dans le cadre des formalités de demande de visa et d'immigration. Le mémoire déposé par le Commissariat portait également sur un article visant à soustraire le *Registre des armes d'épaule* de l'application de la *Loi sur la protection des renseignements personnels*.

Vérifications

En vertu de la *Loi sur la protection des renseignements personnels*, le Commissariat a toute latitude pour examiner les pratiques de protection de la vie privée des institutions fédérales et recommander au besoin des mesures correctives.

VÉRIFICATION DES PRATIQUES DE TRAITEMENT DES RENSEIGNEMENTS PERSONNELS DANS LE CADRE DU PROGRAMME DE LA SÉCURITÉ DE LA VIEILLESSE

L'administration du Programme de la sécurité de la vieillesse (SV) requiert la collecte d'une grande quantité de renseignements personnels sensibles, depuis le numéro d'assurance sociale jusqu'aux données financières. En février 2015, le Commissariat a entrepris la vérification des pratiques d'Emploi et Développement social Canada (EDSC) en matière de traitement des renseignements personnels pour les besoins du Programme de la SV. Il s'est également penché sur le rôle joué par Services partagés Canada (SPC) dans la protection de l'infrastructure de TI dans laquelle sont stockés les renseignements de la SV.

En général, comme il est indiqué dans la version intégrale du rapport de vérification, même si EDSC s'est doté de nombreux éléments propres à un régime efficace de gestion de la vie privée, nous avons constaté bien des lacunes et des points faibles dans la mise en œuvre de certaines de ses politiques et pratiques de sécurité et de protection de la vie privée, entre autres :

- L'entente opérationnelle actuelle conclue entre EDSC et SPC, qui décrit en termes généraux leur relation soutenue, ne définit pas le rôle et les responsabilités des deux ministères en ce qui concerne la protection des renseignements personnels des bénéficiaires de la SV – que le Secrétariat du Conseil du Trésor (SCT) considère pourtant comme un « élément essentiel » de ce type d'ententes. Or, en l'absence d'une entente définissant clairement la façon dont les renseignements personnels seront protégés, il y a un risque de consultation, d'utilisation ou de communication inappropriée de ces renseignements. Le Commissariat a recommandé qu'EDSC collabore avec SPC afin d'élaborer une entente prévoyant des dispositions adéquates pour assurer la sécurité et protéger la vie privée.

- En examinant de nombreuses ententes d'échange de renseignements (EER) conclues entre EDSC et ses partenaires, le Commissariat a constaté que certaines ne contenaient pas les dispositions clés en matière de sécurité et de protection de la vie privée. Il a donc recommandé à EDSC de mettre à jour ses ententes en utilisant son gabarit d'EER le plus récent, qui

renferme des dispositions permettant de combler les lacunes observées.

- Ni les systèmes de la SV gérés par EDSC ni l'infrastructure qui les héberge n'ont été accrédités et certifiés comme il se doit. En conséquence, les risques d'atteinte à la vie privée et à la sécurité des TI n'ont pas été pleinement évalués et atténués. Le Commissariat a recommandé à EDSC d'évaluer les risques associés à ces systèmes dans le cadre du processus de certification et d'accréditation, comme l'exige la politique du SCT. Il lui a aussi recommandé de collaborer avec SPC afin que l'infrastructure fasse l'objet des évaluations requises.

- EDSC a mis en place des procédures pour s'assurer que les renseignements personnels sont consultés uniquement par les employés ayant un besoin légitime de savoir. Toutefois, le Commissariat a constaté que ces procédures n'étaient pas toujours suivies et qu'aucune surveillance proactive n'était exercée pour savoir qui a accédé à des renseignements personnels dans les systèmes de TI et à quel moment on y a accédé. Nous avons recommandé à EDSC de respecter ses propres procédures et d'examiner régulièrement les pistes de vérification produites par les systèmes de TI concernant les activités des utilisateurs dans les systèmes de la SV.

- La version papier de dossiers fermés de bénéficiaires de la SV était conservée au-delà de la période de six ans prescrite par la politique d'EDSC. Quant aux dossiers électroniques, ils sont actuellement conservés indéfiniment, mais le Ministère met actuellement en œuvre un calendrier de conservation et d'élimination pour lui permettre de les détruire. Le Commissariat a recommandé à EDSC d'élaborer un plan d'élimination des dossiers qui ont été conservés au-delà de la limite de six ans.

- Les mesures de contrôle de la sécurité physique des documents papier stockés étaient adéquates dans les locaux visités par le Commissariat. Par ailleurs, EDSC assure maintenant le suivi des évaluations de la menace et des risques (EMR) afin de mieux gérer les résultats de ces évaluations. Les EMR ne sont pas effectuées à une fréquence uniforme à EDSC, et il n'y a aucune surveillance centralisée pour s'assurer que les risques d'atteinte à la sécurité physique sont évalués et atténués de façon uniforme à l'échelle nationale. Le Commissariat a recommandé à EDSC de mettre à jour sa politique de sécurité actuelle pour y indiquer la fréquence à laquelle les EMR devraient avoir lieu et d'établir une fonction de surveillance centralisée.

EDSC a pris connaissance des conclusions issues de notre vérification et il est d'accord avec toutes nos recommandations. Le Ministère s'est engagé à mettre en place des mesures précises et à respecter des échéanciers à cette fin. On trouvera dans le rapport de vérification la réponse complète d'EDSC. La vérification portait sur les pratiques de gestion des renseignements personnels au sein d'EDSC, mais le Commissariat s'est aussi intéressé dans ce contexte aux lacunes constatées concernant SPC.

Le Commissariat n'a pas le pouvoir d'exiger la mise en œuvre de ses recommandations, mais il assure un suivi après deux ans pour déterminer quelles mesures ont été prises afin d'y donner suite.

Suivi de travaux antérieurs

Le Commissariat a fait le suivi de sa vérification de 2013 de l'Agence du revenu du Canada (ARC) afin de déterminer quelles mesures l'Agence avait prises pour mettre en œuvre ses recommandations et veiller à ce que les renseignements personnels des contribuables soient protégés le mieux possible contre toute consultation, utilisation ou communication interne inappropriée.

L'ARC a affirmé avoir mis en œuvre en totalité ou en grande partie toutes les mesures recommandées par le Commissariat. Elle a indiqué avoir apporté plusieurs améliorations importantes à son mode de gestion des renseignements personnels, notamment en adoptant de nouvelles politiques, en renforçant la surveillance ministérielle et en veillant à la réalisation d'une évaluation des risques d'atteinte à la sécurité et à la vie privée en temps plus opportun.

En 2013, l'ARC a nommé un chef de la protection des renseignements personnels (CPRP), qui est investi d'un vaste mandat au chapitre de la surveillance et de la promotion de la protection de la vie privée. Le CPRP, qui siège au Comité de gestion de l'Agence, doit notamment superviser les décisions relatives à la protection de la vie privée, y compris les évaluations des facteurs relatifs à la vie privée (EFVP); défendre le droit des individus à la vie privée, y compris la gestion des atteintes à la vie privée; et superviser la sensibilisation à la protection de la vie privée, y compris les activités de communication et de formation à l'intention de tous les employés de l'ARC.

L'ARC a aussi amélioré ses mesures de contrôle applicables aux technologies de l'information (TI) pour les systèmes touchant les contribuables, y compris la gestion et la surveillance des droits d'accès internes. Elle devrait terminer en 2017 la mise en œuvre intégrale des contrôles de surveillance recommandés dans notre rapport de vérification. L'ARC a investi à ce jour environ 10,5 millions de dollars et prévoit un autre investissement important afin d'améliorer les contrôles de gestion de l'identité et de l'accès. Enfin, l'Agence a amélioré ses procédures en cas d'atteinte à la vie privée afin d'accélérer la déclaration d'incidents.

Évaluation des facteurs relatifs à la vie privée

Le SCT oblige les institutions fédérales à effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) pour les activités ou programmes nouveaux ou ayant subi des modifications importantes qui sont appelés à utiliser des renseignements personnels pour prendre des décisions touchant des individus. Les institutions doivent fournir une copie de leurs EFVP au Commissariat. Nous examinons ces évaluations et, au besoin, nous informons l'institution concernée des risques d'atteinte à la vie privée et des mesures à prendre pour améliorer ses pratiques de traitement des renseignements personnels. Même si les recommandations du Commissariat ne sont pas contraignantes, les institutions les acceptent et les mettent en œuvre dans la majorité des cas.

On trouvera quelques exemples ci-après :

Gendarmerie royale du Canada – Caméras vidéo corporelles

La GRC évalue actuellement la possibilité de mettre en œuvre un programme national qui obligerait tous ses membres à porter une caméra vidéo corporelle sur leur uniforme.

À l'heure actuelle, ces caméras servent à l'occasion, habituellement sur le site de protestations ou de manifestations où la GRC craint des actes de violence.

Le Commissariat continue de consulter la GRC sur cette question. Il a formulé des recommandations encourageant la GRC à faire preuve de transparence dans son utilisation des caméras vidéo corporelles et à veiller à ce que leur utilisation soit nécessaire et proportionnée avant de se déployer dans une situation donnée. Nous nous attendons à être tenus pleinement informés de tout développement concernant ce programme, y compris de toute utilisation envisagée de logiciels de reconnaissance faciale ou de tout autre type d'analyse vidéo.

Échange de renseignements entre l'Agence du revenu du Canada et l'Internal Revenue Service des États-Unis

Après avoir examiné l'EFVP de l'Agence du revenu du Canada (ARC) portant sur l'administration de l'Accord intergouvernemental (AIG) en vertu de la *Foreign Account Tax Compliance Act* (FATCA) des États-Unis, le Commissariat a soulevé de nombreuses préoccupations auprès de l'Agence. L'AIG prévoit la collecte, auprès des institutions financières canadiennes, de renseignements personnels concernant des comptes déclarables appartenant à des entités ou des citoyens américains et leur transmission par l'ARC à l'Internal Revenue Service (IRS) des États-Unis.

Dans son examen initial, le Commissariat a noté la possibilité d'une collecte excessive de renseignements personnels. Il a exprimé des préoccupations au sujet du manque de clarté concernant le seuil pour la déclaration de comptes ayant un solde de 50 000 $ ou plus et de la période de conservation de 11 ans qui lui semblait inutilement longue.

Dans sa réponse, l'ARC a accepté de ramener à sept ans la période de conservation (ce qui correspond à sa période de conservation des déclarations de revenus des particuliers) et de créer un formulaire Web pour s'assurer que les institutions financières fournissent uniquement les renseignements nécessaires afin de réduire le risque de collecte excessive. L'Agence a aussi clarifié les dispositions se rapportant au seuil de 50 000 $. Elle a précisé que la *Loi de l'impôt sur le revenu* autorise les institutions financières à décider d'appliquer ou non ce seuil, tandis que l'AIG les autorise à choisir de ne pas l'appliquer. Bref, en théorie, les institutions doivent signaler tous les comptes, mais elles peuvent choisir d'appliquer le seuil dans certaines situations.

L'ARC a également fait savoir au Commissariat qu'elle valide les renseignements déclarés afin de s'assurer qu'ils sont complets et uniformes pour les besoins de l'évaluation des risques, mais elle ne dispose pas des données voulues pour vérifier si les comptes déclarables ont été signalés comme il se doit. Pour faciliter l'accès des personnes aux renseignements les concernant et leur permettre d'exprimer leur désaccord si elles estiment que ceux-ci ont été transférés à tort, le Commissariat a recommandé que l'ARC envisage d'aviser les personnes touchées lorsque leurs renseignements sont transmis à l'IRS.

Programme de soutien par les pairs en santé mentale de l'Agence canadienne d'inspection des aliments

En juin 2015, l'Agence canadienne d'inspection des aliments (ACIA) a lancé un programme à participation volontaire en vertu

duquel les employés ayant des problèmes de santé mentale peuvent communiquer avec des collègues qui ont surmonté des difficultés similaires. Cette initiative part d'une bonne intention, mais elle soulève de nombreuses questions et préoccupations en matière de protection de la vie privée.

L'EFVP n'a pas permis de déterminer clairement comment les collègues apportant leur soutien protégeraient les renseignements personnels des participants et leur anonymat ni comment on s'y prendrait dans la pratique pour prévenir la communication inappropriée d'information. Nous avons recommandé à l'ACIA de mettre à jour son EFVP afin d'inclure, entre autres, une évaluation visant à déterminer si les politiques et procédures du programme donnent des orientations suffisantes pour assurer la conformité à la *Loi sur la protection des renseignements personnels* et une évaluation des mesures techniques et des contrôles de sécurité destinés à atténuer les risques d'atteinte à la vie privée.

L'ACIA a répondu à notre lettre de recommandations et a accepté la plupart des mesures préconisées, mais elle continue de limiter la portée de l'EFVP à un examen des risques pour les renseignements personnels des pairs aidants, et non des participants. Le Commissariat continue de recommander à l'ACIA de modifier son EFVP de façon à y inclure une analyse plus complète des risques d'atteinte à la sécurité des renseignements sensibles communiqués par les participants.

Plaintes et enquêtes

ENQUÊTES EN VERTU DE LA LPRPDE

Au cours des cinq derniers exercices, le nombre de plaintes déposées en vertu de la LPRPDE a augmenté, mais davantage de plaintes ont été fermées à l'issue d'un règlement rapide et les délais de traitement ont grandement diminué.

Entre le 1er janvier 2015 et le 31 mars 2016, le Commissariat a accepté 391 plaintes en vertu de la LPRPDE. Comme nous l'avons indiqué dans le message du commissaire, une modification législative apportée en 2015 a modifié le cycle de production de rapports concernant la LPRPDE, qui correspondait auparavant à une année civile, pour adopter un cycle correspondant à l'exercice. Aux fins de comparaison, le Commissariat avait accepté 309 plaintes en 2015, ce qui représente une hausse de 49 % par rapport aux 207 plaintes acceptées en 2010.

En 2015, le Commissariat a fermé 171 dossiers à l'issue d'un règlement rapide, soit plus de deux fois plus qu'en 2010 (80). Pendant la même période, 133 dossiers ont été fermés à l'issue d'une enquête ordinaire, soit près de deux fois moins que les 249 dossiers fermés de cette façon en 2010. Entre 2010 et 2015, le délai de traitement moyen a été ramené de trois mois à 2,7 mois pour les dossiers fermés à l'issue d'un règlement rapide et il a été réduit considérablement, soit de 19,2 mois à 12,2 mois pour les dossiers fermés à l'issue d'une enquête ordinaire.

Les chapitres précédents portaient sur des enquêtes clés menées en vertu de la LPRPDE, mais nous sommes en mesure de faire part des détails de dossiers uniquement dans les rapports au Parlement et en ajoutons fréquemment de nouveaux sur notre site Web à l'adresse https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/.

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

Depuis cinq ans, on enregistre une augmentation du nombre de plaintes en vertu de la *Loi sur la protection des renseignements personnels* reçues par le Commissariat. Cette hausse s'explique par les nouvelles technologies et l'intégration des programmes gouvernementaux, qui donnent lieu à un accroissement des échanges de renseignements personnels des Canadiens et ajoutent à la complexité des enquêtes. Le Commissariat a eu davantage recours à la procédure de règlement rapide et a mis en œuvre des stratégies pour composer avec les plaintes multiples reçues par suite d'un seul incident et aux plaintes multiples déposées par une même personne. Cette approche a entraîné des gains d'efficience, si bien que des milliers de Canadiens ont pu se prévaloir de recours chaque année. Le Commissariat arrive toutefois à un point où il ne peut plus suivre le rythme des demandes.

En 2015-2016, le Commissariat a accepté 1 768 plaintes en vertu de la *Loi sur la protection des renseignements personnels*, comparativement à 3 977 au cours de l'exercice précédent. Toutefois, si l'on exclut les dossiers où une même personne a déposé des plaintes multiples (qui, selon notre stratégie de traitement des plaintes multiples, demeurent en instance, ce qui nous permet de répondre plus équitablement aux besoins d'un ensemble plus large de plaignants), le nombre de plaintes – qui est plus représentatif de notre charge de travail – a en fait augmenté, passant de 1 040 à 1 389. Par rapport à il y a cinq ans (2010-2011), le nombre de plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels* a augmenté de 96 %.

Le Commissariat a eu beaucoup plus souvent recours à la procédure de règlement rapide au cours des cinq derniers exercices. En 2015-2016, il a fermé 1 226 dossiers en vertu de la *Loi sur la protection des renseignements personnels*, dont 460 à l'issue d'un règlement rapide. Ces chiffres représentent une hausse marquée par rapport à 2010-2011, alors que 648 dossiers avaient été fermés (hausse de 89 % en cinq ans), dont seulement 78 à l'issue d'un règlement rapide (hausse de 489 % en cinq ans). Le délai de traitement moyen des dossiers fermés à l'issue d'un règlement rapide a également diminué en cinq ans, passant de 3,6 à 2,2 mois. Toutefois, en ce qui concerne les dossiers fermés à l'issue d'une enquête ordinaire, le délai de traitement moyen a augmenté, passant est passé de huit à un peu plus de dix mois, notamment en raison d'une hausse constante du nombre de dossiers complexes.

Comme nous l'avons mentionné au chapitre 1, le Commissariat peut donner les détails des enquêtes menées en vertu de la *Loi sur la protection des renseignements personnels* uniquement dans les rapports au Parlement. Le résumé de dossiers de l'exercice écoulé est présenté ci-après. La version complète de ces cas et d'autres rapports de conclusions d'enquêtes est affichée sur notre site Web.

Une émission de télévision soulève de nombreuses questions relatives au consentement

Depuis 2012, l'Agence des services frontaliers du Canada (ASFC) participait à une émission télévisée intitulée *Douanes sous haute surveillance : Canada.* Toutes les semaines, on y présentait le travail des agents de l'ASFC, le plus souvent lorsqu'ils interrogeaient des voyageurs sélectionnés pour une inspection

secondaire. Avant le début du tournage, un agent de l'ASFC demandait aux individus l'autorisation de les filmer. Une fois le tournage terminé – et en supposant que les voyageurs avaient donné leur consentement verbal –, la société de production leur demandait de signer un formulaire de consentement l'autorisant à utiliser pour l'émission les séquences tournées. Ces individus renonçaient ainsi aux droits que leur confère la *Loi sur la protection des renseignements personnels*. On brouillait le visage de ceux qui refusaient de donner leur consentement.

L'enquête du Commissariat a porté à la fois sur le tournage de l'arrestation d'un plaignant à l'occasion d'une descente de l'ASFC sur un chantier de construction dans la région de Vancouver en 2012 et sur des enjeux plus vastes concernant l'émission. À l'issue de son enquête, le Commissariat a soulevé de nombreuses préoccupations concernant le respect de la vie privée, la plus importante ayant trait au consentement :

- Puisque l'ASFC avait autorisé la société de production à pénétrer dans les zones de contrôle des douanes pour y filmer ses activités, elle lui a communiqué des renseignements personnels en temps réel. Or, pour qu'une communication dans ces conditions soit conforme à la *Loi sur la protection des renseignements personnels,* l'ASFC devait obtenir le consentement valide et valable des personnes concernées.

- Le Commissariat n'a pas été convaincu que l'ASFC avait obtenu ce consentement. De nombreux facteurs, dont la contrainte, ont eu une incidence sur la validité du consentement, qui doit être donné librement, de façon volontaire et en toute connaissance de cause. En raison du caractère coercitif d'une détention par l'ASFC, il est possible que les personnes détenues n'aient pas été dans l'état d'esprit voulu pour donner un consentement vraiment volontaire.

- En examinant les séquences vidéo brutes où figure le plaignant – et contrairement à ce qu'alléguait l'ASFC –, le Commissariat a constaté que le tournage avait commencé avant que l'on tente d'obtenir un consentement. L'agent de l'ASFC a posé plusieurs questions au plaignant avant de l'informer des fins du tournage.

- Même si le plaignant a signé par la suite le formulaire de consentement, le Commissariat n'a trouvé aucune preuve indiquant qu'on lui avait bien expliqué – ainsi qu'à d'autres – la signification de la renonciation aux droits que lui confère la *Loi sur la protection des renseignements personnels* ni qu'on lui avait offert la possibilité d'obtenir un avis juridique indépendant avant de signer le formulaire de consentement.

- Le Commissariat a aussi soulevé des préoccupations concernant les techniques de brouillage utilisées pour cacher l'identité des personnes. Le niveau de brouillage utilisé le plus souvent était faible et il y avait une abondance de renseignements secondaires, si bien qu'il était fort possible que les téléspectateurs puissent identifier les personnes.

Dans la conclusion de notre enquête, nous avons rappelé à l'ASFC que la protection de la vie privée doit être l'un des principaux facteurs à prendre en compte dans l'élaboration initiale et l'administration de ce type d'initiative. En réponse aux conclusions et aux

recommandations du Commissariat, l'ASFC a mis fin à sa participation à l'émission. L'Agence a aussi pris acte de la recommandation l'encourageant à effectuer à l'avenir une évaluation des facteurs relatifs à la vie privée avant de participer à une émission télévisée.

L'Agence du revenu du Canada prend des mesures adéquates pour empêcher le transfert de renseignements personnels aux États-Unis

Une fois que nos renseignements personnels quittent le Canada – qu'ils soient transférés par une institution fédérale ou une organisation du secteur privé ou encore que nous les ayons transférés nous-mêmes –, ils sont dès lors régis par les lois du pays où ils se trouvent. Ces lois détermineront qui peut y avoir accès. Dans certains cas, les lois étrangères peuvent autoriser l'accès à nos renseignements personnels dans des situations ou à des fins que nombre d'entre nous pourraient trouver contestables par rapport aux lois canadiennes sur la protection des renseignements personnels.

Dans ce dossier, le plaignant s'inquiétait du fait que l'Agence du revenu du Canada (ARC) avait confié le stockage des dossiers fiscaux des Canadiens à une entreprise qu'il croyait établie aux États-Unis. Si c'était le cas, les autorités américaines pourraient avoir accès aux renseignements personnels des contribuables canadiens en vertu de la *PATRIOT Act* des États-Unis.

En mai 2013, l'ARC a accordé un contrat à Mobilshred Inc. pour le stockage et la gestion des dossiers fiscaux des Canadiens. Au cours de ses discussions avec l'ARC et les dirigeants de Mobilshred Inc., faisant affaire sous le nom de « Recall », le Commissariat a déterminé que Mobilshred Inc. est détenue à 100 % par Recall Canada Holdings, entité canadienne elle-même détenue à 100 % par la société mère de Recall, Recall Holdings Limited, qui a son siège en Australie. Le Commissariat a constaté que Mobilshred Inc. ne possède aucun établissement aux États-Unis.

À la lumière de notre enquête, nous avons conclu que l'ARC avait pris les mesures appropriées pour prévenir l'éventuelle communication des renseignements fiscaux de contribuables canadiens aux autorités américaines. Entre autres, son contrat avec Mobilshred renferme une exigence selon laquelle tous les renseignements transférés à l'entreprise – tous en format papier – demeurent au Canada en tout temps.

Par ailleurs, nous avons aussi constaté que l'ARC, avant d'accorder le contrat, avait communiqué avec sa Direction de l'accès à l'information et de la protection des renseignements personnels, le Commissariat et le ministère de la Justice pour s'assurer qu'elle avait bien pris en compte et résolu toutes les questions liées à la sécurité et à la protection de la vie privée, y compris en ce qui a trait à la *PATRIOT Act* des États-Unis.

La collecte de signatures électroniques par Postes Canada pour assurer le suivi du courrier fait l'objet d'une plainte

Postes Canada recueille régulièrement la signature électronique des individus lorsqu'ils acceptent un envoi postal pour lequel l'expéditeur a demandé une preuve de livraison. Pour autant que le destinataire ne s'y oppose pas, sa signature est affichée sur le site Web de Postes Canada, où l'expéditeur peut la voir en tapant le numéro de suivi de l'envoi en question.

Dans ce dossier, le plaignant alléguait que Postes Canada n'en faisait pas assez pour s'assurer que les destinataires d'un envoi comprennent bien qu'ils peuvent refuser que leur signature soit affichée en ligne (auquel cas l'expéditeur pouvait demander une copie papier). Une étiquette indiquant que le destinataire accepte que sa signature soit vue en ligne est apposée sur les appareils utilisés par Postes Canada pour enregistrer les signatures électroniques.

À l'issue de notre examen, nous avons conclu que la communication des signatures aux fins de suivi des envois correspondait aux fins auxquelles Postes Canada les avait recueillies au départ. En conséquence, rien n'oblige Postes Canada à obtenir un consentement pour communiquer une signature – même sur son site de suivi en ligne. Le Commissariat a soulevé des préoccupations concernant le fait que le libellé de l'étiquette sur les appareils à signature n'était peut-être pas assez clair. Pour sa part, Postes Canada considérait que la procédure permettant aux clients de refuser que leur signature soit affichée en ligne était claire et bien comprise et n'a pas accepté de modifier le texte. À notre avis, Postes Canada ne contrevient pas pour autant à la Loi.

Toutefois, nous nous sommes également penchés sur l'outil de suivi en ligne utilisé par Postes Canada. Après avoir examiné les mesures de sécurité et de protection de la vie privée mises en place pour protéger les signatures numérisées affichées en ligne, nous n'étions pas convaincus que Postes Canada avait analysé adéquatement les risques associés aux fonctions et à la conception du site pour protéger adéquatement les signatures des destinataires.

Postes Canada s'est donc engagée à mieux sécuriser son site de suivi en ligne, notamment en mettant en œuvre le protocole HTTPS, plus sûr, afin d'atténuer le risque global d'atteinte à la vie privée. Le Commissariat considère cet aspect de la plainte comme conditionnellement résolu. Postes Canada tiendra le Commissariat au courant des progrès de la mise en œuvre des mesures de contrôles indiquées.

Traitement inadéquat des renseignements personnels des employés

Chaque année, le Commissariat reçoit de nombreuses plaintes déposées contre des institutions fédérales qui auraient autorisé une consultation ou une communication inappropriées des renseignements personnels de leurs employés. Voici quelques exemples :

- La Commission des libérations conditionnelles du Canada (CLCC) a négligé d'examiner attentivement certains documents, si bien que les renseignements médicaux d'un employé ont été communiqués à de nombreuses personnes qui devaient participer à une audience sur une question de dotation. Nous avons noté que, dans sa demande de renseignements sur le processus de nomination, le Tribunal de la dotation de la fonction publique (maintenant intégré à la Commission des relations de travail et de l'emploi dans la fonction publique) avait informé la CLCC que les renseignements personnels, y compris les renseignements médicaux et les renseignements sur la santé, devaient être retirés de tous les documents avant qu'ils soient transmis au Tribunal.

- Une employée de Travaux publics et Services gouvernementaux Canada (aujourd'hui Services publics et Approvisionnement Canada) s'est plainte

du fait qu'une gestionnaire contre laquelle elle avait déposé une plainte pour harcèlement en avait informé des personnes qui n'avaient aucun besoin de connaître cette information au cours d'une réunion du personnel. La gestionnaire avait alors communiqué non seulement ses propres renseignements personnels, mais aussi des renseignements personnels sensibles concernant l'employée. Cette affaire rappelle qu'il faut indiquer aux personnes mises en cause dans des procédures de recours qu'elles doivent faire preuve de la plus grande discrétion.

- Au cours d'un exercice de formation sur la saisie de données à la GRC, on a remis aux participants diverses données à saisir dans un système de suivi des plaintes pour harcèlement en milieu de travail. Ces données comprenaient le nom, le rang, l'adresse et les coordonnées de plaignants, une description du harcèlement allégué ainsi que le nom des autres personnes en cause. Une des employées en formation a constaté que les renseignements n'étaient pas génériques, comme elle s'y attendait, mais qu'ils se rapportaient à des plaintes réelles. D'après l'enquête du Commissariat, le surintendant de la GRC responsable de la séance de formation avait décidé d'utiliser de véritables données dans le but de réduire un arriéré dans la saisie des données. Il avait communiqué par le fait même des renseignements personnels sensibles concernant des dizaines d'employés.

Atteintes à la sécurité des données

NOUVELLE HAUSSE DU NOMBRE D'ATTEINTES À LA SÉCURITÉ DES DONNÉES DÉCLARÉES EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le nombre d'atteintes à la vie privée déclarées au Commissariat augmente d'année en année, en particulier depuis 2014, année où le Secrétariat du Conseil du Trésor a adopté une politique obligeant les institutions fédérales à déclarer les atteintes substantielles à la vie privée. Malheureusement, sans les fonds supplémentaires nécessaires, notre capacité à traiter efficacement ces déclarations est limitée. À l'heure actuelle, nous devons nous contenter de procéder de façon superficielle lors de nos examens, de nos avis et de nos suivis dans la grande majorité des incidents déclarés.

En 2015-2016, le nombre d'incidents déclarés au Commissariat est passé de 256 à 298, soit une hausse de 16 % par rapport à l'exercice précédent. Comme par le passé, les « communications accidentelles » ont été la principale cause des atteintes à la vie privée, ce qui fait ressortir la nécessité pour les institutions d'adopter des procédures appropriées pour protéger les renseignements personnels des Canadiens.

Nul ne peut nier que la directive administrative rendant obligatoire la déclaration des incidents a amélioré les choses, mais certaines institutions ne déclarent toujours pas les atteintes à la vie privée. La plupart des incidents déclarés l'an dernier l'ont été par une poignée d'organisations. Comme on peut le voir à l'annexe 2, plusieurs organisations détenant d'énormes quantités de renseignements personnels ont déclaré très peu d'incidents.

En avril 2016, l'information déposée à la Chambre des communes en réponse à une question posée par un député a donné lieu à d'autres questions concernant l'uniformité des déclarations d'une institution fédérale à l'autre. Selon cette information, plus de 5 800 atteintes à la vie privée avaient été enregistrées en 2015-2016 et à peine un peu plus de 5 % avaient été déclarées au Commissariat.

Lorsque nous avons dû répondre à des questions à ce sujet, nous avons fait observer que nombre des atteintes ne portaient pas nécessairement sur des renseignements personnels ou sur des données suffisamment sensibles pour être considérées comme des atteintes « substantielles ». Dans ces circonstances, il n'était donc pas nécessaire de déclarer ces incidents en vertu de la politique du Conseil du Trésor.

Comme nous l'avons mentionné au chapitre 1, si une disposition législative obligeait les institutions fédérales à déclarer expressément les atteintes « substantielles » à la vie privée, le Commissariat aurait une idée plus précise de la situation dans l'ensemble des institutions fédérales et serait mieux placé pour collaborer avec les organisations afin de les aider à atténuer les risques et les répercussions.

DÉCLARATION DES ATTEINTES À LA SÉCURITÉ DES DONNÉES EN VERTU DE LA LPRPDE ET MISE EN ŒUVRE DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS NUMÉRIQUES*

Le nombre de déclarations volontaires d'atteintes à la sécurité des données au Commissariat par des organisations assujetties à la LPRPDE a augmenté en flèche au cours du dernier exercice. Nous en avons reçu 98 pendant l'année civile 2015, soit plus du double par rapport aux 44 incidents déclarés en 2014.

Cette hausse du nombre d'incidents déclarés pourrait indiquer que les entreprises se préparent à une nouvelle réalité, car la déclaration – aux Canadiens et au Commissariat – des atteintes à la sécurité des données présentant un véritable risque de préjudice important pour les individus deviendra bientôt obligatoire.

Ce changement découle de l'adoption de la *Loi sur la protection des renseignements personnels numériques* (projet de loi S-4) en juin 2015. Le régime de déclaration obligatoire des atteintes à la sécurité des données n'entrera pas en vigueur avant qu'Innovation, Sciences et Développement économique Canada ait terminé de rédiger le règlement d'application connexe, mais d'autres modifications sont entrées en vigueur immédiatement. Une fiche d'information publiée par le Commissariat en 2015 explique toutes les modifications.

Coopération internationale et nationale

Le Commissariat a maintenu sa longue tradition de promotion du droit à la vie privée et de la connaissance de ce domaine sur la scène internationale en continuant de participer à diverses tribunes et en collaborant avec des organismes analogues de partout dans le monde. Au cours de l'exercice écoulé, nous avons notamment contribué à l'élaboration de documents de travail publiés par le Groupe de travail international sur la protection des données dans les télécommunications. Mentionnons un document portant sur les rapports de transparence et un sur les accessoires intelligents à porter sur soi, tous deux publiés en avril 2015.

CONFÉRENCE INTERNATIONALE DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE – RÉSOLUTION SUR LA TRANSPARENCE

À l'occasion de la Conférence internationale des commissaires à la protection des données et de la vie privée qui s'est tenue en octobre 2015 à Amsterdam, nos homologues d'autres pays ont appuyé une résolution sur la transparence (coparrainée par le commissariat de la Nouvelle-Zélande) visant les fournisseurs de services de télécommunications qui reçoivent des demandes de renseignements personnels émanant d'institutions gouvernementales.

Cette résolution exhorte les organisations du secteur privé à publier des rapports de transparence concernant le nombre de demandes qu'ils reçoivent, la nature de leurs réponses et les motifs juridiques sur lesquels les institutions gouvernementales se basent pour demander accès aux renseignements personnels de leurs clients et employés. La résolution exhorte aussi les gouvernements à tenir des dossiers exacts et à faire rapport publiquement sur la nature, le but et le nombre de demandes d'accès licite qu'ils présentent et à éliminer les obstacles aux rapports de transparence.

Outre la résolution sur les rapports de transparence, la conférence d'Amsterdam a mené à d'autres résolutions : un engagement de coopération avec le Rapporteur spécial des Nations Unies sur le droit à la vie privée et un appui aux analyses et aux orientations nécessaires en lien avec la vie privée et les actions humanitaires internationales, par exemple dans le cadre des efforts visant à aider les personnes déplacées dans les situations de violence et de catastrophes naturelles.

LEADERSHIP ET PARTICIPATION À DES TRIBUNES INTERNATIONALES

Tout au long de l'exercice, le Commissariat a continué de s'acquitter de ses responsabilités en tant que nouveau membre du Comité exécutif de la Conférence internationale des commissaires à la protection des données et de la vie privée. Il a également continué d'assurer la coprésidence du Common Thread Network qui, dans un communiqué publié en novembre 2015, exhortait les chefs de gouvernement du Commonwealth à accorder une plus grande priorité à la protection de la vie privée. L'organisation a souligné que le Commonwealth est bien placé pour apporter une valeur ajoutée à la protection des données et de la vie privée à l'échelle internationale. Dans un communiqué publié plus tard le même mois à l'issue de leur rencontre, les chefs de gouvernement ont reconnu la nécessité d'adopter des cadres juridiques qui protègent le droit à la vie privée et résolu d'encourager le développement de réseaux pratiques facilitant l'échange d'information et le renforcement des capacités dans le domaine de la protection des données et de la vie privée.

Le Commissariat est aussi membre du groupe des autorités de protection de la vie privée de la zone Asie-Pacifique, qui a tenu son 43e forum à Hong Kong en juin 2015 et son 44e forum à Macao en décembre 2015, ainsi que de l'Association francophone des autorités de protection des données personnelles (AFAPDP), qui a adopté une résolution sur la surveillance de masse et, comme nous l'avons mentionné au chapitre 5, une résolution sur la prise en compte des principes éthiques dans le traitement des données à caractère personnel dans le domaine de la santé et de la génétique.

ORIENTATIONS SUR LES PROGRAMMES « APPORTEZ VOTRE PROPRE APPAREIL »

Le Commissariat travaille également en étroite collaboration avec ses partenaires provinciaux et territoriaux et prend part régulièrement à des consultations continues. Par exemple, au cours de l'exercice écoulé, nous avons collaboré avec les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique afin d'élaborer et de publier des lignes directrices à l'intention des organisations qui envisagent d'autoriser leurs employés à apporter leur propre appareil mobile au travail. Il s'agit d'une pratique de plus en plus répandue.

Cette pratique prend de l'ampleur, mais elle estompe la ligne de démarcation entre la vie personnelle et la vie professionnelle. Les employés commencent à s'inquiéter du risque d'atteinte à leur vie privée, sans parler des enjeux associés à la collecte et à l'utilisation des renseignements personnels des consommateurs qui pourraient se retrouver dans les téléphones cellulaires et les autres appareils mobiles des employés.

Programme des contributions

Créé en 2004 pour appuyer la recherche indépendante et sans but lucratif sur la protection de la vie privée, encourager l'élaboration de politiques en la matière et promouvoir la protection des renseignements personnels au Canada, le Programme des contributions est considéré comme l'un des meilleurs programmes au monde pour le financement de la recherche dans le domaine. Le Commissariat lance chaque année un appel de propositions ainsi que, certaines années, un appel de propositions spécial pour des projets d'application des connaissances de la série Parcours de protection de la vie privée, qui s'appuient sur des recherches déjà menées à bien. Ce programme, que le gouvernement du Canada a récemment renouvelé pour une autre période de cinq ans, est doté d'un budget annuel de 500 000 $. Chaque projet peut recevoir un financement maximal de 50 000 $.

Ce programme a contribué à l'avancement de nos priorités stratégiques en favorisant l'adoption de solutions novatrices face à des enjeux nouveaux ou émergents ayant des répercussions sur la vie privée. Les projets retenus pour un financement et les autres annonces en lien avec le Programme des contributions sont affichés sur notre site Web. Cette année, neuf projets directement liés aux priorités stratégiques du Commissariat en matière de protection de la vie privée ont été réalisés, et 10 demandes ont été retenues pour l'exercice

2016-2017. En outre, de nombreux projets récents ont été présentés en détail dans le dernier numéro de notre publication intitulée *Résultats réels*.

Devant les tribunaux

Au cours de l'exercice écoulé, le Commissariat a témoigné dans le cadre d'interventions ou de requêtes liées à de nombreux dossiers :

Fontaine et autre c. Canada
L'an dernier, la Cour d'appel de l'Ontario a autorisé le Commissariat à intervenir devant les tribunaux et ce dernier a témoigné dans le cas d'appels et d'appels incidents liés à la protection, à l'archivage et à l'élimination éventuelle de dossiers créés dans le cadre du Processus d'évaluation indépendant (PEI) en lien avec la Convention de règlement

relative aux pensionnats indiens (CRRPI). Sans prendre position officiellement sur le fond, le Commissariat s'est demandé si le degré de confidentialité 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 en vertu de la Convention. Le Commissariat a aussi présenté des mémoires concernant les facteurs à prendre en compte afin de déterminer si les dossiers du PEI relèvent du gouvernement. Il a aussi souligné l'importance pour les survivants des pensionnats de conserver le contrôle de leur propre histoire individuelle.

Les juges de la Cour ont statué majoritairement que les dossiers du PEI ne relèvent pas du gouvernement et qu'ils ne sont donc pas assujettis à la *Loi sur la protection des renseignements personnels,* ni à la *Loi sur l'accès à l'information,* ni à la *Loi sur la Bibliothèque et les Archives du Canada*. Les juges ont aussi maintenu à la majorité l'ordonnance en vertu de laquelle les documents devront être détruits après une période de conservation de 15 ans. Ils ont précisé que, pendant cette période, les documents seront assujettis aux dispositions de confidentialité de la CRRPI, mais non aux lois fédérales sur l'accès à l'information et la protection des renseignements personnels.

La décision a des répercussions importantes compte tenu des plaintes déjà déposées auprès du Commissariat et de celles qui pourraient l'être par la suite concernant le traitement réservé aux dossiers du PEI par le Secrétariat du PEI. La Cour suprême du Canada a été saisie d'une demande d'autorisation d'interjeter appel de cette décision.

The Information and Privacy Commissioner of Alberta v. The Board of Governors of the University of Calgary

Le Commissariat à la protection de la vie privée du Canada, le Commissariat à l'information et divers autres commissariats provinciaux et territoriaux à l'information et à la protection de la vie privée sont intervenus conjointement dans une affaire entendue par la Cour suprême du Canada le 1er avril 2016. Dans cette affaire, la Cour devra déterminer si la commissaire à la protection de la vie privée de l'Alberta peut obtenir des documents à l'égard desquels une entité publique, en l'occurrence une université, revendique le privilège du secret professionnel de l'avocat en vertu de la *Freedom of Information and Protection of Privacy Act* de l'Alberta.

Il s'agit de déterminer ce que doit prévoir un texte de loi pour permettre à un mandataire, par exemple le commissaire à la protection de la vie privée, d'avoir préséance sur le secret professionnel de l'avocat dans le but d'examiner une plainte. Le libellé en question est très semblable à celui contenu dans la *Loi sur la protection des renseignements personnels*, selon lequel « nonobstant toute autre loi fédérale ou toute immunité reconnue par le droit de la preuve, le Commissaire à la protection de la vie privée a, pour les enquêtes qu'il mène en vertu de la présente loi, accès à tous les renseignements, quels que soient leur forme et leur support, qui relèvent d'une institution fédérale, à l'exception des renseignements confidentiels du Conseil privé de la Reine pour le Canada ».

Aucune décision n'avait encore été rendue au moment de la rédaction du présent rapport.

Banque Royale du Canada c. X et autre
Même s'il n'était pas partie au litige, le Commissariat a participé à une audience devant la Cour d'appel de l'Ontario à titre d'« ami de la Cour ». On lui a alors demandé de jouer le même rôle dans le cadre d'un pourvoi en appel subséquent devant la Cour suprême du Canada. La cause portée en appel (qui a été entendue en avril 2016) vise à déterminer si la LPRPDE empêche un créancier d'obtenir une quittance de remboursement intégral d'une hypothèque consentie par un tiers prêteur à un débiteur dans le but de prendre un recours judiciaire afin d'exécuter un jugement. Les juges de la Cour d'appel de l'Ontario ont statué majoritairement que la LPRPDE empêche en pareil cas la communication sans le consentement et que le consentement implicite était insuffisant.

X c. Canada (Office des transports du Canada) et autre
En juin 2015, la Cour d'appel fédérale a rendu une décision dans une affaire portant sur le principe de la publicité des débats judiciaires tel qu'il s'applique à un tribunal administratif ainsi que sur le concept des renseignements personnels « auxquels le public a accès » en vertu de la *Loi sur la protection des renseignements personnels*. Le Commissariat avait le statut d'intervenant.

Selon la Cour, le principe de la publicité des débats judiciaires s'applique à l'Office des transports du Canada (OTC) dans sa fonction en tant que tribunal quasi judiciaire. Le règlement de l'organisme précise clairement que l'Office devrait « verse[r] dans ses archives publiques les documents concernant une instance qui sont déposés auprès de lui », sauf si une demande de traitement confidentiel a été déposée. La Cour a statué que les documents demandés par le requérant avaient été versés dans les archives publiques de l'OTC comme l'exigent ses règles et que tous ces documents étaient par conséquent des documents « auxquels le public a accès » au sens de la *Loi sur la protection des renseignements personnels*. Par conséquent, l'OTC a reçu l'ordre de communiquer les documents non expurgés, conformément à la demande du requérant.

Cette décision s'appliquait à l'OTC, mais le Commissariat continue d'encourager les tribunaux administratifs, qui ont chacun leurs propres règles, pouvoirs et attributions, à adopter des politiques qui, tout en respectant le principe de la publicité des débats judiciaires et les particularités de leur loi habilitante, respectent aussi leurs obligations en matière de protection de la vie privée en vertu de la *Loi sur la protection des renseignements personnels*.

X c. Procureur général du Canada
L'an dernier, le Commissariat a été autorisé à intervenir dans une demande de contrôle judiciaire présentée à la Cour fédérale au sujet d'un rapport de conclusions d'enquête publié par le Commissariat à la suite d'une plainte déposée contre l'Agence du revenu du Canada. La requérante met en doute l'équité de notre enquête et les conclusions énoncées dans le rapport.

X c. Commissariat à la protection de la vie privée du Canada
La Cour fédérale a été saisie d'une demande de contrôle judiciaire des constatations du Commissariat relativement à une plainte déposée contre un ministère fédéral en vertu de la *Loi sur la protection des renseignements personnels*. Selon la requérante, les conclusions de notre rapport contiendraient des erreurs et le Commissariat ne lui aurait pas laissé suffisamment l'occasion de faire valoir ses arguments, n'aurait pas mené une enquête

approfondie et n'aurait pas été impartial dans son enquête.

La Cour a rejeté la demande en soulignant que l'enquête du Commissariat avait été approfondie et juste. Elle a également confirmé que le Commissariat devrait jouir d'une grande latitude dans la manière dont il mène ses enquêtes et que l'on ne s'attend pas à ce que les enquêtes et les motifs soient parfaits, mais plutôt à ce qu'ils soient raisonnables.

X et Globe24h.com

Une demande a été présentée en vertu de l'article 14 de la LPRPDE contre le site Web Globe24h.com à la suite de la publication du rapport de conclusions d'enquête du Commissariat (inclus dans le rapport annuel de 2014 sur la LPRPDE) concernant ce site. Le requérant fait partie des 27 plaignants dont les plaintes ont été examinées par le Commissariat. Ce requérant demande réparation contre Globe24h, y compris des dommages-intérêts et une ordonnance pour que le site efface de ses serveurs toutes les décisions des cours et des tribunaux canadiens et qu'il prenne les mesures nécessaires pour supprimer ces décisions des mémoires caches des moteurs de recherche.

En mars 2016, la Cour fédérale a autorisé le Commissariat à participer à l'instance pour fournir de l'information sur l'application de la LPRPDE. Cette instance soulève certaines questions, notamment la mesure dans laquelle la LPRPDE s'applique à un site Web basé à l'étranger; la signification de l'expression « auxquels le public a accès » au sens de la Loi; l'interprétation de l'exclusion « à des fins journalistiques »; et la restriction portant sur les fins acceptables prévue au paragraphe 5(3) de la *Loi*.

Annexe 1 – Définitions

Types de plaintes

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.

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 les renseignements pour en faire état.

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.

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

Répertoire : *InfoSource* (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.

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.

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

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.

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

Délais : L'institution n'aurait pas répondu à une demande dans les délais prescrits par la *Loi sur la protection des renseignements personnels*.

Avis de prorogation : Sous le régime 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.

Correction ou annotation (délais) : Sous le régime 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 dans les 30 jours suivant la réception de la demande de correction pour en faire état.

Responsabilité : Sous le régime 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.

Possibilité de porter plainte : Sous le régime 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.

Consentement : Sous le régime de la LPRPDE, une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement valable de la personne concernée 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.

Transparence : Sous le régime de la LPRPDE, une organisation n'a pas rendu facilement accessibles aux personnes des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Mesures de protection : Sous le régime de la LPRPDE, une organisation n'a pas protégé par des mesures de protection appropriées les renseignements personnels qu'elle détient.

Détermination des fins de la collecte des renseignements : Sous le régime 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.

Décisions

Fondée : L'institution ou l'organisation a enfreint une disposition 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, mais elle 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 : Sous le régime 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, 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 concernées et n'a publié aucune conclusion.

Abandonnée :

> **Sous le régime de la *Loi sur la protection des renseignements personnels*** : L'enquête a pris fin avant que l'on ait pleinement examiné toutes les allégations. 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.
>
> **Sous le régime de la LPRPDE :** L'enquête a pris fin sans qu'une conclusion 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. 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 ne publie aucune conclusion.

Refus d'enquêter : Sous le régime 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 : Sous le régime de la LPRPDE, **l**e 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

Plaintes en vertu de la LPRPDE acceptées, par secteur de l'industrie (du 1er janvier 2015 au 31 mars 2016)

Secteur de l'industrie	Nombre	Proportion par rapport à l'ensemble des plaintes acceptées
Assurances	32	8 %
But non lucratif	1	0 %
Divertissement	4	1 %
Finances	57	15 %
Gouvernement	11	3 %
Hébergement	15	4 %
Internet	83	22 %
Services	38	10 %
Services professionnels	6	2 %
Télécommunications	46	12 %
Transports	26	7 %
Vente et commerce de détail	28	7 %
Autres secteurs	34	9 %
Total	381	100 %

Plaintes en vertu de la LPRPDE acceptées, par type de plainte (du 1er janvier 2015 au 31 mars 2016)

Type de plainte	Nombre	Proportion par rapport à l'ensemble des plaintes acceptées
Accès	79	21 %
Collecte	20	5 %
Consentement	124	33 %
Conservation	5	1 %
Correction ou annotation	9	2 %
Exactitude	7	2 %
Fins appropriées	9	2 %
Mesures de protection	39	10 %
Responsabilité	4	1 %
Transparence	2	1 %
Utilisation et communication	83	22 %
Total	381	100 %

Enquêtes en vertu de la LPRPDE fermées, par secteur de l'industrie et décision (du 1er janvier 2015 au 31 mars 2016)

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	28		1		5		10		10	4	30	58
Gouvernement	7					1					1	8
Sans but lucratif	1										0	1
Transports	12	1			1	1	2		5	2	12	24
Télécommunications	41				2		2	1	4	1	10	51
Services	19	1			1				1	1	4	23
Internet	34		3		4	1		2	2		12	46
Assurances	12	1	4	4	3	1	2		1	2	18	30
Vente et commerce de détail	22		1		3	2		2	4	2	14	36
Hébergement	9			1	1		1		1		4	13
Services professionnels	6							1	2		3	9
Divertissement	3								1		1	4
Autres secteurs	36	2	3		2	1	1		3		12	48
Total	230	5	12	5	22	7	18	6	34	12	121	351

Enquêtes en vertu de la LPRPDE fermées, par type de plainte et décision (du 1er janvier 2015 au 31 mars 2016)

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	45	3	2	1	5	1	2	1	11	2	73
Utilisation et communication	53	6		2	1		3	4	10	6	85
Collecte	19		1	2	4	2	2		3	1	34
Fins appropriées	3	1			2		1				7
Mesures de protection	27		2		4	1	2		2	2	40
Consentement	66	2			6	1	7	1	8	1	92
Exactitude	3						1				4
Conservation	5										5
Responsabilité	1					2					3
Correction ou annotation	6										6
Transparence	2										2
Frais											0
Total	230	12	5	5	22	7	18	6	34	12	351

Enquêtes en vertu de la LPRPDE – Délais de traitement moyens, par décision (du 1er janvier 2015 au 31 mars 2016)

Décision	Nombre	Délai de traitement moyen (en mois)
Résolue par règlement rapide	230	2,9
Réglée	7	5,4
Abandonnée (art. 12.2)	12	9,6
Retirée	22	15,3
Hors du champ d'application	5	2,1
Non fondée	18	14,0
Fondée et conditionnellement résolue	12	23,0
Fondée et résolue	34	16,1
Fondée	6	14,8
Refus d'enquêter	5	4,2
Total	351	
Moyenne générale pondérée		**6,7**

Enquêtes en vertu de la LPRPDE – Délais de traitement moyens, par type de plainte et de règlement (du 1er janvier 2015 au 31 mars 2016)

	Règlement rapide		Autres règlements (sauf règlement rapide)		Ensemble des 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	45	3,0	28	11,2	73	6,1
Collecte	19	3,2	15	13,8	34	7,9
Consentement	66	2,8	26	14,6	92	6,1
Conservation	5	3,4			5	3,4
Correction ou annotation	6	1,1			6	1,1
Exactitude	3	2,8	1	19,3	4	6,9
Fins appropriées	3	2,4	4	10,6	7	7,1
Mesures de protection	27	2,9	13	10,2	40	5,3
Responsabilité	1	5,3	2	4,3	3	4,6
Transparence	2	2,8			2	2,8
Utilisation et communication	53	3,0	32	13,2	85	6,8
Total	**230**	**2,9**	**121**	**12,6**	**351**	**6,7**

Déclarations volontaires des atteintes en vertu de la LPRPDE, par secteur de l'industrie et type d'incident (du 1er janvier 2015 au 31 mars 2016)

	Type d'incident			Total des incidents par secteur de l'industrie	Proportion par rapport à l'ensemble des incidents
Secteur de l'industrie	Communication accidentelle	Perte	Vol et accès non autorisé		
Assurances	1		4	5	4 %
Divertissement	1		1	2	2 %
Finances	17	1	13	31	27 %
Gouvernement			1	1	1 %
Hébergement			2	2	2 %
Internet			3	3	3 %
Organismes sans but lucratif	3		4	7	6 %
Santé	6		2	8	7 %
Services	4	2	8	14	12 %
Télécommunications	7		2	9	8 %
Transports	1		2	3	3 %
Vente et commerce de détail	2	1	16	19	17 %
Autres secteurs	1		10	11	10 %
Total	**43**	**4**	**68**	**115**	100 %

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

Intimé	Fondée	Fondée et résolue	Non fondée	Résolue	Abandonnée	Résolue par règlement rapide	Réglée	Total
Administration canadienne de la sûreté du transport aérien							1	1
Affaires autochtones et du Nord Canada	1							1
Affaires mondiales Canada			1			7		8
Agence canadienne d'inspection des aliments			1			2		3
Agence de la santé publique du Canada						3		3
Agence des services frontaliers du Canada		2	11	1	3	32		49
Agence du revenu du Canada	11	5	9	1	57	12		95
Anciens Combattants Canada		2	1			6		9
Banque du Canada						1		1
Bureau de l'ombudsman de l'approvisionnement			1					1
Bureau du Conseil privé						10		10
Centre de la sécurité des télécommunications			1	1				2
Comité de surveillance des activités de renseignement de sécurité						2		2
Commissariat à l'information du Canada			1					1
Commissariat à l'intégrité du secteur public du Canada	1		4					5
Commissariat à la protection de la vie privée du Canada			1					1
Commissariat au lobbying du Canada						1		1
Commissariat aux langues officielles						2		2
Commission canadienne d'examen des exportations de biens culturels		1						1
Commission canadienne de sûreté nucléaire	1							1
Commission canadienne des droits de la personne			1					1
Commission de l'immigration et du statut de réfugié du Canada			1			3		4
Commission de la fonction publique du Canada	1	4	1		2			8
Commission des champs de bataille nationaux								0
Commission des libérations conditionnelles du Canada	1		4		1	6		12
Conseil de la radiodiffusion et des télécommunications canadiennes						2		2
Conseil national de recherches Canada			1					1
École de la fonction publique du Canada				2		1		3
Élections Canada			1		1	8		10
Emploi et Développement social Canada	2		6	1		24	1	34
Environnement et Changement climatique Canada			1			4		5

Décisions sur les plaintes relatives à l'accès et à la protection des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*, par institution (suite)

Intimé	Fondée	Fondée et résolue	Non fondée	Résolue	Abandonnée	Résolue par règlement rapide	Réglée	Total
Gendarmerie royale du Canada	6	6	19	1	16	58	1	107
Immigration, Réfugiés et Citoyenneté Canada	1	1	5		2	20		29
Infrastructure Canada		1						1
Innovation, Sciences et Développement économique Canada			3			4		7
Instituts de recherche en santé du Canada						1		1
Justice Canada	1	3	4		7	10		25
Ministère de la Défense nationale			19	1	5	18	1	44
Office des transports du Canada						1		1
Passeport Canada	1		1			1		3
Patrimoine canadien						1		1
Pêches et Océans Canada	1				1	2		4
Ressources naturelles Canada						2		2
Santé Canada		2	22	1	2	13		40
Secrétariat du Conseil du Trésor du Canada						8		8
Sécurité publique Canada						2		2
Service Canada					1	4		5
Service canadien du renseignement de sécurité			16			6	3	25
Service correctionnel du Canada	9	12	14	3	13	87	3	141
Service des poursuites pénales du Canada		1	2			1		4
Services publics et Approvisionnement Canada	1	1			1	8	1	12
Société canadienne des postes			5		4	12		21
Société Radio-Canada			9			3		12
Statistique Canada				1	1	2		4
Technologies du développement durable du Canada						1		1
Transports Canada		2				7		9
VIA Rail Canada					1			1
Total	**38**	**43**	**166**	**13**	**118**	**398**	**11**	**787**

Délais de traitement des plaintes en vertu de la *Loi sur la protection des renseignements personnels* – Règlement rapide, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen (en mois)
Accès		
Accès	255	2,38
Correction ou annotation	2	3,87
Langue	1	1,49
Délais		
Délais	61	1,10
Correction – Délais		
Avis de prorogation	1	0,40
Protection des renseignements personnels		
Utilisation et communication	113	2,45
Collecte	16	1,86
Conservation et retrait	7	1,56
Exactitude	4	3,75
Total	**460**	**2,21**

Délais de traitement en vertu de la *Loi sur la protection des renseignements personnels* – Enquêtes ordinaires, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen (en mois)
Accès		
Accès*	160	18,74
Correction ou annotation	1	17,27
Délais		
Délais	323	4,82
Correction – Délais	2	2,78
Avis de prorogation	52	3,15
Protection des renseignements personnels		
Utilisation et communication*	71	17,78
Collecte	10	16,54
Conservation et retrait	7	14,96
Exactitude	2	12,25
Total	**628**	**10,03**

* Comprend une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 138.

Délais de traitement en vertu de la *Loi sur la protection des renseignements personnels* – Tous les dossiers fermés, par décision

Type de plainte	Nombre	Délai de traitement moyen (en mois)
Plaintes ordinaires*		
Fondée*	319	5,98
Non fondée	176	13,07
Abandonnée	69	9,15
Fondée et résolue	41	24,32
Réglée	9	25,67
Résolue	14	15,21
Résolue par règlement rapide	460	2,21
Total	**1 088**	**6,70**

* Comprend une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 138.

Atteintes en vertu de la *Loi sur la protection des renseignements personnels*, par institution

Intimé	Incident
Administration canadienne de la sûreté du transport aérien	1
Affaires autochtones et du Nord Canada	9
Affaires mondiales Canada	7
Agence canadienne d'évaluation environnementale	1
Agence des services frontaliers du Canada	1
Agence du revenu du Canada	21
Anciens Combattants Canada	84
Centre de la sécurité des télécommunications Canada	2
Comité externe d'examen des griefs militaires	1
Commissariat à l'information du Canada	1
Commission canadienne des droits de la personne	1
Commission de la fonction publique du Canada	10
Élections Canada	3
Emploi et Développement social Canada	17
Environnement et Changement climatique Canada	1
Gendarmerie royale du Canada	12
Immigration, Réfugiés et Citoyenneté Canada	47
Justice Canada	3
Ministère de la Défense nationale	1
Musée canadien de l'histoire	1
Pêches et Océans Canada	4
Santé Canada	2
Service canadien du renseignement de sécurité	1
Service correctionnel du Canada	50
Service des poursuites pénales du Canada	5
Services publics et Approvisionnement Canada	4
Statistique Canada	4
Transports Canada	3
VIA Rail Canada	1
Total	**298**

Plaintes en vertu de la Loi sur la protection des renseignements personnels

Catégorie	Total
Acceptées	
Accès	418
Délais	478
Protection des renseignements personnels	493
Total – Acceptées et en cours	**1 389**
Total – Acceptées et en suspens	379
Fermées à la suite d'un processus de règlement rapide	
Accès	258
Délais	62
Protection des renseignements personnels	140
Total	**460**
Fermées à la suite d'une enquête ordinaire	
Accès	210
Délais	377
Protection des renseignements personnels	179
Total	**766**
Total – Fermées	**1 226**
Plaintes pour atteinte reçues	
Communication accidentelle	242
Vol	5
Perte	29
Accès non autorisé	22
Total – Reçues	**298**

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées, par type de plainte*

Type de plainte	Règlement rapide		Enquête		Nombre total	Pourcentage total
	Nombre	Pourcentage	Nombre	Pourcentage		
Accès						
Accès	299	55 %	104	12 %	403	29 %
Correction ou annotation	5	1 %	1	0 %	6	0 %
Langue	9	2 %	0	0 %	9	1 %
Délais						
Délais	55	10 %	352	42 %	407	29 %
Prorogation	1	0 %	66	8 %	67	5 %
Correction – Délais	0	0 %	4	0 %	4	0 %
Protection des renseignements personnels						
Utilisation et communication	132	24 %	97	11 %	229	17 %
Collecte	25	5 %	220	26 %	245	18 %
Conservation et retrait	10	2 %	5	1 %	15	1 %
Exactitude	4	1 %	0	0 %	4	0 %
Total	540	100 %	849	100 %	1 389	100 %

* N'inclut pas les plaintes en suspens (379)

Les dix institutions visées par le plus grand nombre de plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées

Intimé	Accès		Délais		Protection des renseignements personnels		Total
	Règlement rapide	Enquête	Règlement rapide	Enquête	Règlement rapide	Enquête	
Service correctionnel du Canada	94	12	34	178	21	208	547
Gendarmerie royale du Canada	48	9	4	34	15	10	120
Agence des services frontaliers du Canada	34	12	3	29	7	3	88
Agence du revenu du Canada	9	8	0	15	10	43	85
Ministère de la Défense nationale	11	12	3	40	6	5	77
Commission de la fonction publique du Canada	0	5	0	60	0	9	74
Immigration, Réfugiés et Citoyenneté Canada	13	4	0	11	10	6	44
Emploi et Développement social Canada	14	1	4	5	15	3	42
Service canadien du renseignement de sécurité	8	16	4	0	0	3	31
Environnement et Changement climatique Canada	11	0	0	10	1	0	22
Secrétariat du Conseil du Trésor du Canada	7	1	0	9	0	5	22
Total	**249**	**80**	**52**	**391**	**85**	**295**	**1 152**

Les dix institutions visées par le plus grand nombre de plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées, par exercice financier

Institution	2012-2013	2013-2014	2014-2015	2015-2016
Service correctionnel du Canada	284	514	314	547
Gendarmerie royale du Canada	182	265	140	120
Agence des services frontaliers du Canada	88	56	66	88
Agence du revenu du Canada	76	61	106	85
Ministère de la Défense nationale	90	84	68	77
Commission de la fonction publique du Canada	3	6	2	74
Immigration, Réfugiés et Citoyenneté Canada	17	53	42	44
Emploi et Développement social Canada	1 030	78	35	42
Service canadien du renseignement de sécurité	19	17	21	31
Environnement et Changement climatique Canada	2	1	7	22
Secrétariat du Conseil du Trésor du Canada	2	1	3	22
Total	**1 793**	**1 136**	**804**	**1 152**

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées, par institution

Intimé	Règlement rapide	Enquête	Total
Affaires autochtones et du Nord Canada	0	10	10
Affaires mondiales Canada	8	4	12
Agence canadienne d'inspection des aliments	2	1	3
Agence de la santé publique du Canada	5	0	5
Agence des services frontaliers du Canada	44	44	88
Agence du revenu du Canada	19	66	85
Anciens Combattants Canada	8	4	12
Banque du Canada	1	0	1
Bibliothèque et Archives Canada	2	0	2
Bureau du Conseil privé	2	9	11
Bureau du surintendant des institutions financières	1	0	1
Comité de surveillance des activités de renseignement de sécurité	4	0	4
Commissariat à l'intégrité du secteur public du Canada	0	1	1
Commissariat à la protection de la vie privée du Canada	0	1	1
Commissariat aux langues officielles	1	0	1
Commission de l'immigration et du statut de réfugié du Canada	5	0	5
Commission de la fonction publique du Canada	1	73	74
Commission des champs de bataille nationaux	0	1	1
Commission des libérations conditionnelles du Canada	11	7	18
Conseil canadien des normes	1	0	1
Conseil de la radiodiffusion et des télécommunications canadiennes	1	1	2

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées, par institution (suite)

Intimé	Règlement rapide	Enquête	Total
Conseil de recherches en sciences humaines	0	1	1
École de la fonction publique du Canada	0	2	2
Élections Canada	8	2	10
Emploi et Développement social Canada	33	9	42
Environnement et Changement climatique Canada	12	10	22
Finances Canada	0	1	1
Gendarmerie royale du Canada	67	53	120
Immigration, Réfugiés et Citoyenneté Canada	23	21	44
Innovation, Sciences et Développement économique Canada	3	0	3
Instituts de recherche en santé du Canada	2	0	2
Justice Canada	8	9	17
Ministère de la Défense nationale	20	57	77
Office de commercialisation du poisson d'eau douce	0	1	1
Office des transports du Canada	1	0	1
Parcs Canada	3	0	3
Passeport Canada	1	0	1
Patrimoine canadien	1	0	1
Pêches et Océans Canada	3	2	5
Ressources naturelles Canada	2	10	12
Santé Canada	13	0	13
Secrétariat du Conseil du Trésor du Canada	7	15	22
Sécurité publique Canada	2	1	3
Service Canada	8	3	11
Service canadien du renseignement de sécurité	12	19	31
Service correctionnel du Canada	150	397	547
Service des poursuites pénales du Canada	0	3	3
Services partagés Canada	0	1	1
Services publics et Approvisionnement Canada	9	3	12
Société canadienne des postes	11	6	17
Société Radio-Canada	3	1	4
Statistique Canada	4	1	5
Technologies du développement durable du Canada	1	1	2
Transports Canada	10	4	14
Tribunal canadien des droits de la personne	0	1	1
Total	533	856	1 389

Plaintes en vertu de la *Loi sur la protection des renseignements personnels acceptées*, par province ou territoire

Province ou territoire	Règlement rapide		Enquête		Nombre total	Pourcentage total
	Nombre	Pourcentage	Nombre	Pourcentage		
Alberta	49	3,53 %	24	1,73 %	73	5,26 %
Autre (sauf É.-U.)	5	0,36 %	2	0,14 %	7	0,50 %
Colombie-Britannique	100	7,20 %	89	6,41 %	189	13,61 %
États-Unis	5	0,36 %	1	0,07 %	6	0,43 %
Île-du-Prince-Édouard	1	0,07 %	1	0,07 %	2	0,14 %
Manitoba	10	0,72 %	20	1,44 %	30	2,16 %
Non précisé	7	0,50 %	1	0,07 %	8	0,58 %
Nouveau-Brunswick	21	1,51 %	29	2,09 %	50	3,60 %
Nouvelle-Écosse	9	0,65 %	21	1,51 %	30	2,16 %
Nunavut	1	0,07 %	0	0,00 %	1	0,07 %
Ontario	193	13,89 %	456	32,83 %	649	46,72 %
Québec	121	8,71 %	165	11,88 %	286	20,59 %
Saskatchewan	15	1,08 %	31	2,23 %	46	3,31 %
Terre-Neuve-et-Labrador	2	0,14 %	5	0,36 %	7	0,50 %
Territoires du Nord-Ouest	0	0,00 %	0	0,00 %	0	0,00 %
Yukon	0	0,00 %	1	0,07 %	1	0,07 %
Blanc	1	0,07 %	3	0,22 %	4	0,29 %
Total	540	38,88 %	849	61,12 %	1 389	100,00 %

Décisions en vertu de la *Loi sur la protection des renseignements personnels*, par type de plainte

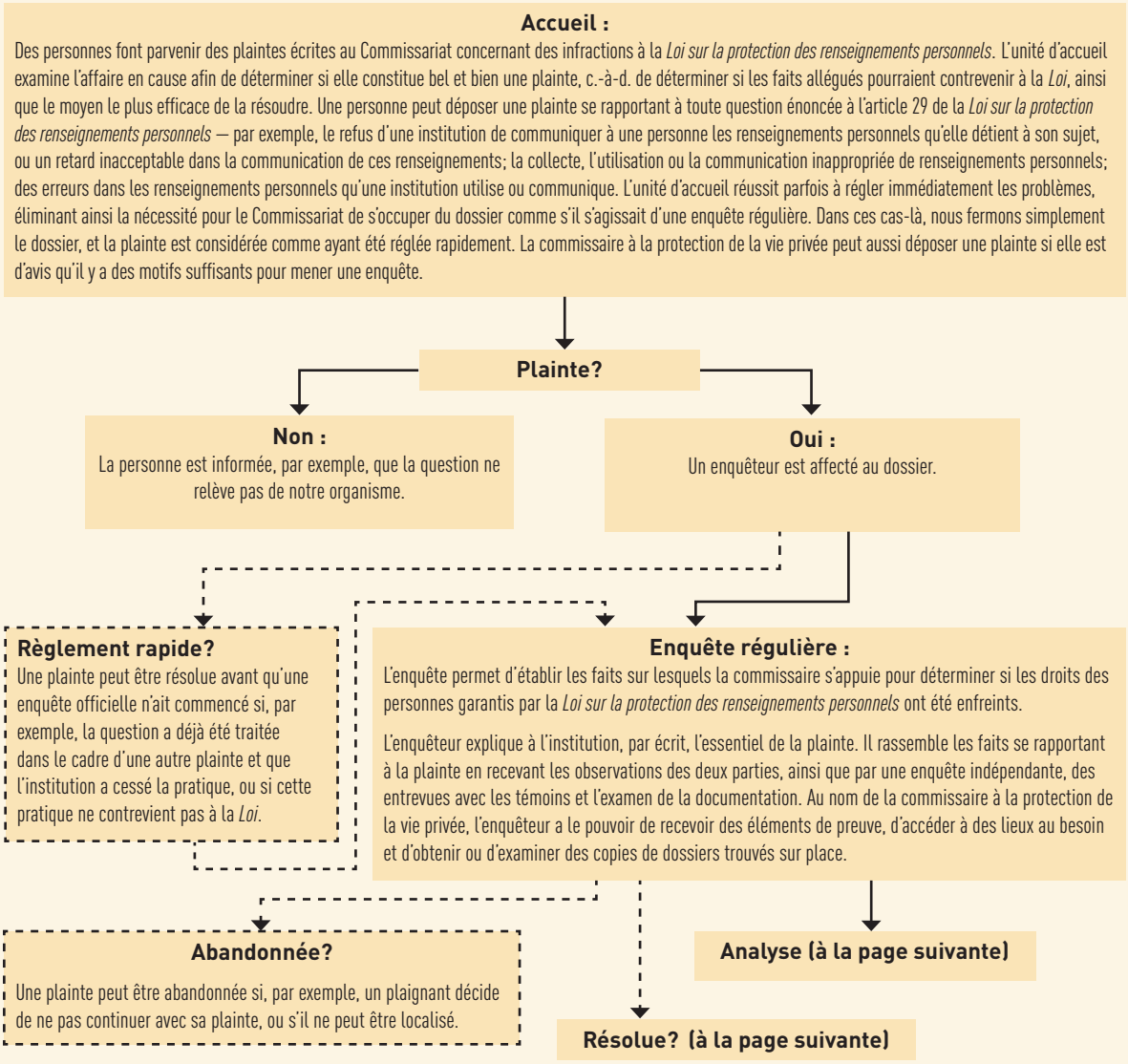
Type de plainte	Fondée	Fondée et résolue	Non fondée	Résolue	Abandonnée	Résolue par règlement rapide	Réglée	Total
Accès								
Accès	6	43	101	12	39	255	8	464
Correction ou annotation				1		2		3
Langue						1		1
Délais								
Délais	280		29	2	12	61		384
Prorogation	10		31		11	1		53
Correction – Délais	2							2
Protection des renseignements personnels								
Utilisation et communication	32		55		70	113	2	272
Collecte			5		5	16	1	27
Conservation et retrait	1		5		1	7		14
Exactitude					2	4		6
Total	**331**	**43**	**226**	**15**	**140**	**460**	**11**	**1 226**

Décisions sur les plaintes relatives aux délais en vertu de la *Loi sur la protection des renseignements personnels*, par institution

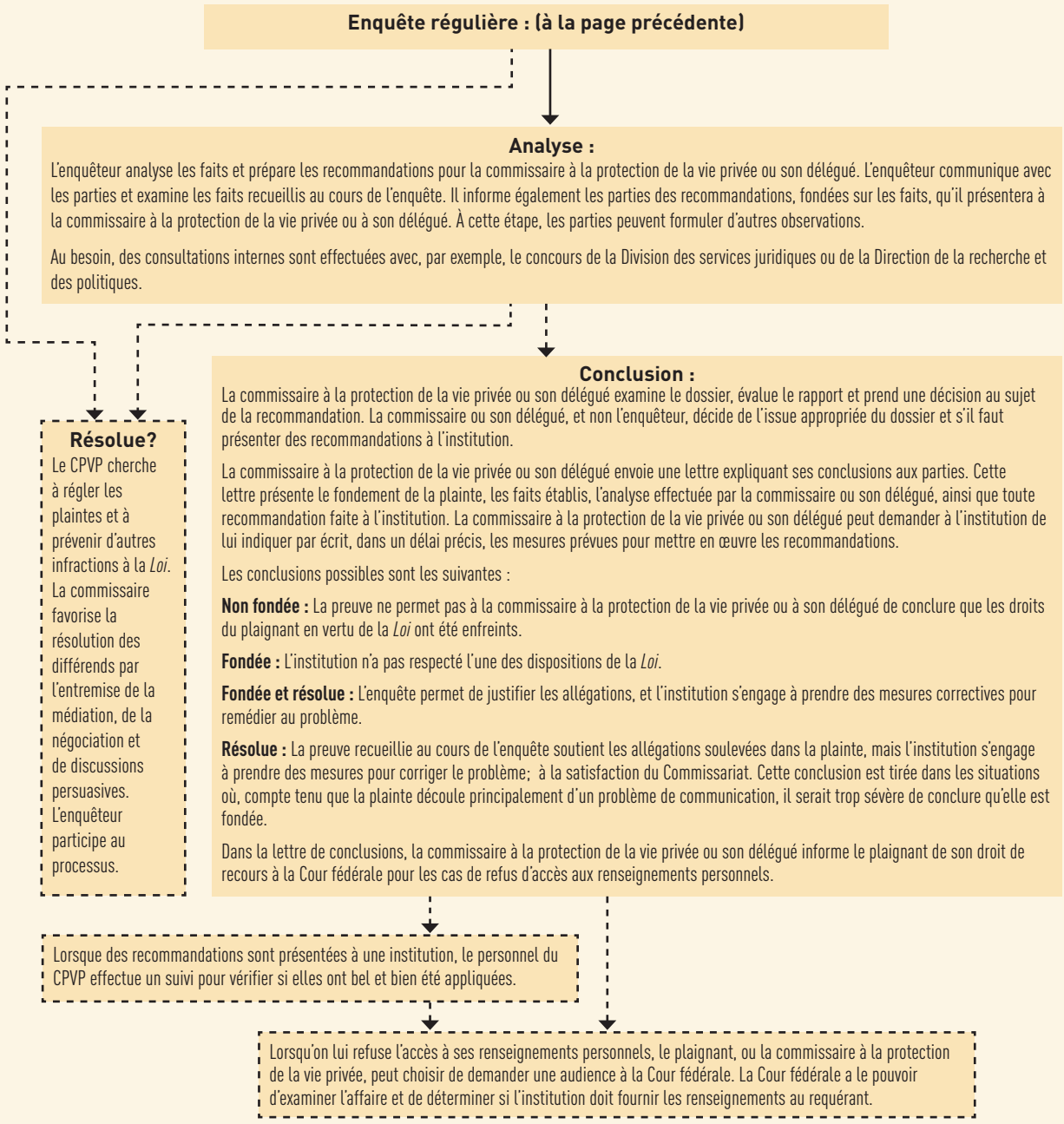
Intimé	Fondée	Fondée et résolue	Non fondée	Résolue	Abandonnée	Résolue par règlement rapide	Total
Affaires mondiales Canada	2				1		3
Agence des services frontaliers du Canada	17		1			3	21
Agence du revenu du Canada	8		1				9
Anciens Combattants Canada	1		1				2
Bureau du Conseil privé			1				1
Commissariat à l'intégrité du secteur public du Canada	1						1
Commission de la fonction publique du Canada	3		36		13		52
Commission des champs de bataille nationaux	1						1
Commission des libérations conditionnelles du Canada	2		2			2	6
Emploi et Développement social Canada	4					4	8
Environnement et Changement climatique Canada	3		6				9
Gendarmerie royale du Canada	24		1			6	31
Immigration, Réfugiés et Citoyenneté Canada	9		1	1	1		12
Instituts de recherche en santé du Canada						1	1
Justice Canada	1		1				2
Ministère de la Défense nationale	29		2		2	3	36
Patrimoine canadien						1	1
Pêches et Océans Canada	2		2		2		6
Ressources naturelles Canada	7		1				8
Secrétariat du Conseil du Trésor du Canada	5		1				6
Service canadien du renseignement de sécurité						4	4
Service correctionnel du Canada	168		2	1	3	38	212
Service des poursuites pénales du Canada			1				1
Services publics et Approvisionnement Canada	3						3
Société canadienne des postes	1						1
Transports Canada	2						2
Total	293		60	2	22	62	439

Annexe 3 – Processus d'enquête

Processus d'enquête – *Loi sur la protection des renseignements personnels*

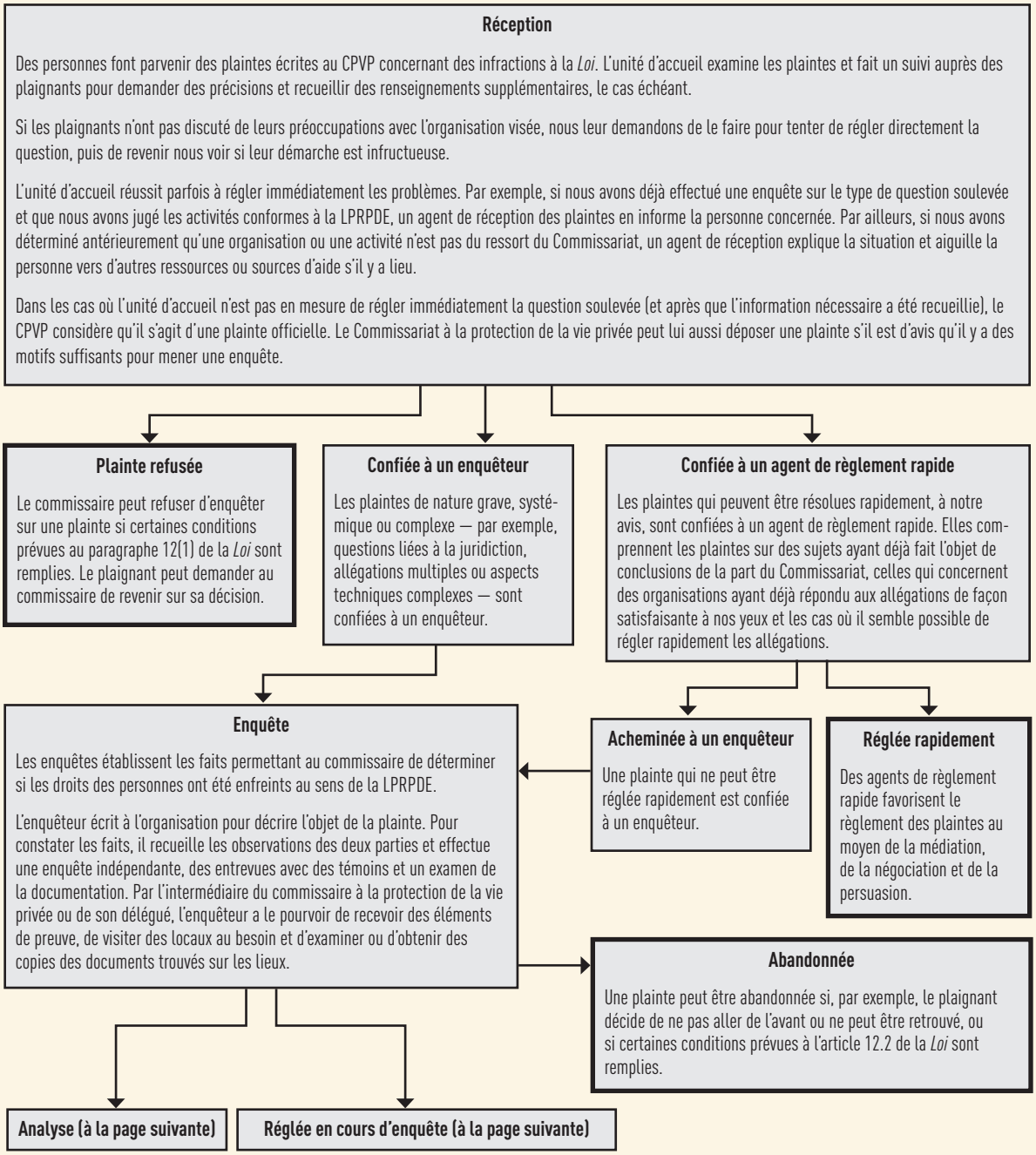


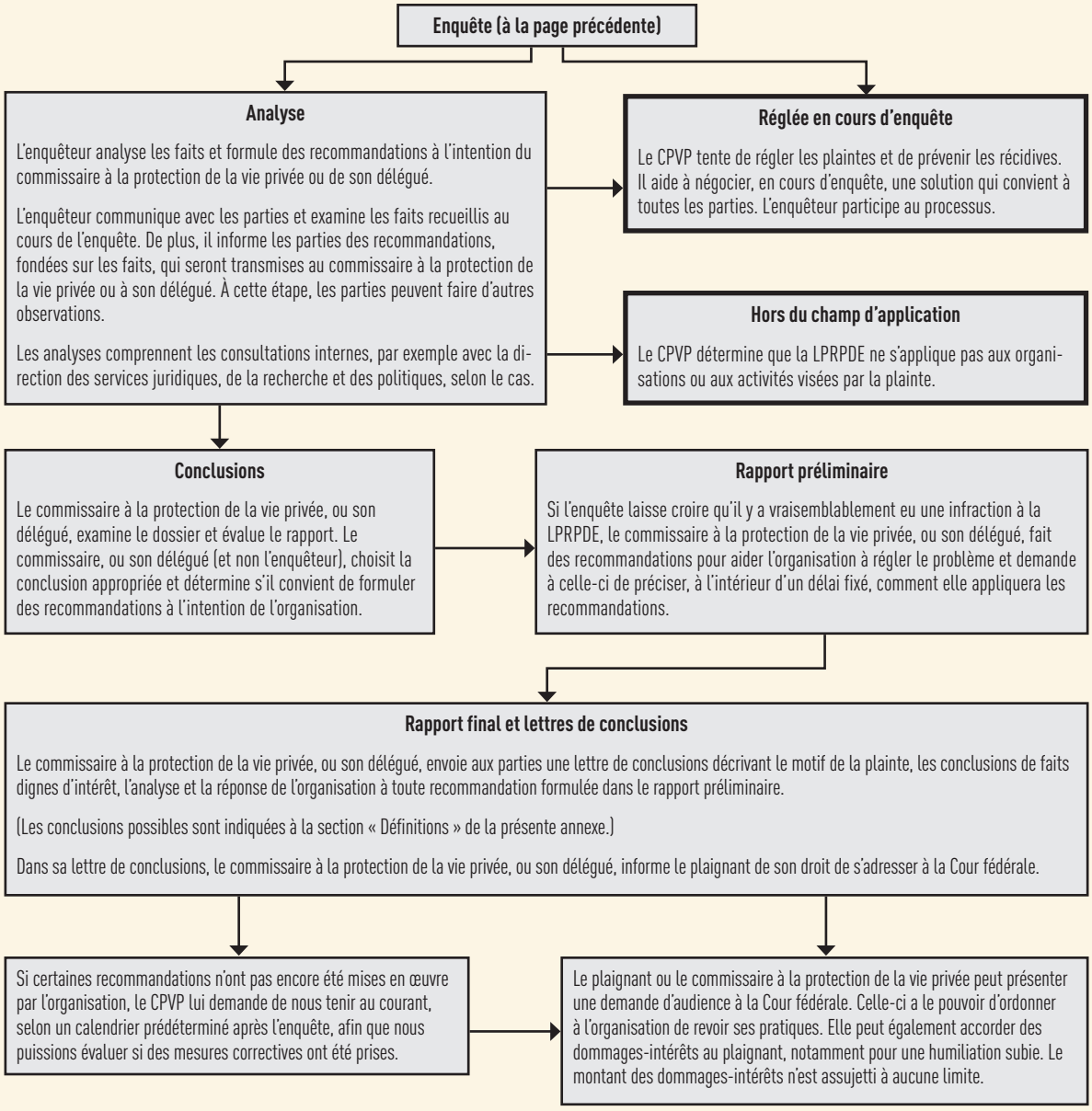
Nota : Une ligne discontinue (- - - -) indique un résultat possible.



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

Processus d'enquête – LPRPDE




Enquête (à la page précédente)
Analyse
L'enquêteur analyse les faits et formule des recommandations à l'intention du commissaire à la protection de la vie privée ou de son délégué.
L'enquêteur communique avec les parties et examine les faits recueillis au cours de l'enquête. De plus, il informe les parties des recommandations, fondées sur les faits, qui seront transmises au commissaire à la protection de la vie privée ou à son délégué. À cette étape, les parties peuvent faire d'autres observations.
Les analyses comprennent les consultations internes, par exemple avec la direction des services juridiques, de la recherche et des politiques, selon le cas.
Réglée en cours d'enquête
Le CPVP 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 CPVP détermine que la LPRPDE ne s'applique pas aux organisations ou aux activités visées par la plainte.
Conclusions
Le commissaire à la protection de la vie privée, ou son délégué, examine le dossier et évalue le rapport. Le commissaire, ou son délégué (et non l'enquêteur), choisit la conclusion appropriée et détermine s'il convient de formuler des recommandations à l'intention de l'organisation.
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 une lettre 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 CPVP lui demande de nous tenir au courant, selon un calendrier prédéterminé après l'enquête, afin que nous puissions évaluer si des mesures correctives ont été prises.
Le plaignant ou le commissaire à la protection de la vie privée peut présenter une demande d'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.

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

Rapport du commissaire spécial à la protection de la vie privée pour 2015-2016

J'ai le plaisir de rendre compte des activités du bureau du commissaire spécial à la protection de la vie privée au cours de la période visée par le présent rapport. Depuis le 1er avril 2007, le Commissariat à la protection de la vie privée du Canada 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 Commissariat pour l'examen des plaintes selon lesquelles le Commissariat n'aurait pas traité une demande de renseignements personnels conformément à la loi. Compte tenu du principe fondamental du droit de la protection de la vie privée, en vertu duquel les décisions concernant la communication de renseignements par le gouvernement doivent faire l'objet d'un examen indépendant, on a créé le bureau du commissaire spécial à la protection de la vie privée en lui conférant le pouvoir d'examiner les plaintes déposées contre le Commissariat en tant qu'institution assujettie à la Loi.

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 Commissariat sous le régime de la Loi.

PLAINTES DE L'EXERCICE PRÉCÉDENT NON RÉGLÉES

Deux plaintes déposées au cours de l'exercice précédent n'étaient toujours pas réglées. Elles avaient été déposées à la suite de la perte d'un disque dur portatif en 2014 pendant le déménagement du Commissariat dans ses nouveaux locaux à Gatineau. La première plainte portait sur la période de conservation des renseignements personnels stockés sur le disque dur égaré et la seconde, sur l'omission de protéger des renseignements personnels détenus par le Commissariat. La première plainte a été jugée non fondée et la deuxième, fondée. Mon prédécesseur, le commissaire spécial à la protection de la vie privée John Sims, c.r., a publié au cours du présent exercice un rapport sur ces plaintes. Il en est question un peu plus loin dans mon rapport.

NOUVELLES PLAINTES DÉPOSÉES AU COURS DU PRÉSENT EXERCICE

Vingt-six (26) plaintes ont été déposées au cours de l'exercice couvert par le présent rapport. Vingt-cinq (25) d'entre elles avaient été examinées et fermées avant la fin de l'exercice, tandis que l'autre sera traitée cette année.

Le principal problème signalé dans les 26 plaintes ainsi que dans une autre mentionnée concerne l'application du paragraphe 22.1(1) de la Loi. Cette disposition prévoit une exception en vertu de laquelle le Commissariat est tenu de refuser de communiquer les renseignements personnels qui ont été créés ou obtenus dans le cadre de toute enquête faite par lui ou sous son autorité. Cependant, une fois l'enquête et toutes les procédures connexes terminées, cette exception est partiellement annulée. L'exception ne s'applique alors plus aux documents créés durant l'enquête.

Dans chaque cas, notre enquête a révélé que les documents faisant l'objet de la plainte avaient été obtenus au cours d'enquêtes menées par le Commissariat lui-même. J'ai donc conclu que l'organisme avait appliqué cette exception obligatoire à juste titre lorsqu'il avait refusé de communiquer les documents demandés. En outre, dans certains cas, le Commissariat avait aussi appliqué des exceptions prévues en vertu des articles 26 (renseignements personnels) et 27 (secret professionnel des avocats).

La majorité de ces plaintes ont été jugées non fondées et une a été abandonnée par le plaignant. Dans un dossier où l'article 26 avait été appliqué, le Commissariat a accepté de communiquer des renseignements supplémentaires. La plainte avait dès lors été jugée résolue et fermée.

Outre ces 26 plaintes, mon bureau a reçu deux lettres d'un individu se disant insatisfait de la manière dont la Gendarmerie royale du Canada (GRC) traitait ses demandes d'accès à l'information. Comme le commissaire spécial n'est pas habilité à traiter ce type de dossier, j'ai invité le plaignant à s'adresser au Commissariat concernant ces plaintes contre la GRC.

RAPPORT SPÉCIAL SUR LA PERTE D'UN DISQUE DUR PAR LE COMMISSARIAT

Mon prédécesseur, John Sims, c.r., a fait enquête sur la perte en 2014 d'un disque dur portatif comportant des renseignements personnels sur les employés du Commissariat à la protection de la vie privée du Canada et du Commissariat à l'information du Canada au cours du déménagement du Commissariat dans ses nouveaux locaux à Gatineau. L'incident s'est produit entre le 13 février et le 20 mars 2014.

Le disque dur servait de copie de sauvegarde des données du système financier utilisé par les deux Commissariats pour gérer et prévoir les salaires des employés. Il renfermait donc des renseignements financiers concernant environ 800 personnes de deux organismes, soit des employés en poste et d'anciens employés, pour la période comprise entre 2002 et le 13 février 2014.

Dans ses conclusions, M. Sims a indiqué que le disque dur portatif n'avait pas été consigné adéquatement et n'avait pas fait l'objet d'un suivi approprié en tant que bien; que l'information stockée sur le disque dur externe avait été conservée plus longtemps que la période recommandée; et que certaines politiques du Commissariat à la protection de la vie privée du Canada et du Conseil du Trésor du Canada n'avaient pas été suivies. Rien n'indique que les renseignements personnels stockés sur le disque dur égaré ont été communiqués ou utilisés de façon inappropriée. M. Sims a formulé plusieurs recommandations au Commissariat, qui les a acceptées. Certaines avaient d'ailleurs été mises en œuvre avant même la fin de l'enquête.

CONCLUSION

Le commissaire spécial, qui exerce ses activités en toute indépendance du Commissariat, aide à assurer l'intégrité du traitement des demandes d'accès à l'information personnelle présentées au Commissariat en tant qu'institution. Il contribue ainsi au bon fonctionnement de l'ensemble du système d'accès à l'information personnel au palier fédéral. Mon bureau est heureux de continuer à jouer ce rôle.

Le 1er juin 2016

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