Rapport annuel au Parlement 2014-2015

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET MAINTIEN DE LA CONFIANCE DU PUBLIC

Rapport concernant la *Loi sur la protection des renseignements personnels*

Commissariat
à la protection de
la vie privée du Canada

Rapport annuel au Parlement concernant la *Loi sur la protection des renseignements personnels* — 2014-2015
Protection des renseignements personnels et maintien de la confiance du public

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

819-994-5444 ou 1-800-282-1376

Numéro de catalogue IP50F-PDF

1913-7559

La présente publication est également affichée sur notre site Web à www.priv.gc.ca.
Suivez-vous sur Twitter : @PrivacyPrivee.

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (613) 947-1698
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (613) 947-1698
1-800-282-1376
www.priv.gc.ca

Decembre 2015

L'honorable George Furey, sénateur
Président
Le 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* pour la période du 1er avril 2014 au 31 mars 2015.

Veuillez 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. : (613) 947-1698
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (613) 947-1698
1-800-282-1376
www.priv.gc.ca

Decembre 2015

L'honorable Geoff Regan, C.P., député
Président
Chambres 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* pour la période du 1er avril 2014 au 31 mars 2015.

Veuillez 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

À NOTER : En novembre 2015, certaines institutions fédérales ont changé de nom. Dans le ce rapport , toutes les institutions sont désignées par le nom sous lequel elles opéraient pendant l'année financière 2014-2015.

Message du commissaire

Au moment de ma nomination au début de juin 2014 — quelques semaines après le début de l'exercice 2014-2015, qui fait l'objet du présent rapport —, j'ai affirmé que mon objectif premier serait de permettre aux Canadiens d'exercer un meilleur contrôle sur leurs renseignements personnels.

Nous sommes en présence de progrès technologiques qui ouvrent la voie à une collecte et une analyse des renseignements personnels que nous aurions eu du mal à nous imaginer il y a quelques années à peine. Les institutions fédérales peuvent tirer parti de ces avancées pour améliorer leur rendement, la prestation des services qu'ils offrent à la population canadienne, le maintien de la sécurité publique.

Par ailleurs, les institutions doivent s'assurer que cette collecte et cette utilisation accrues des donnés demeurent conformes à la *Loi sur la protection des renseignements personnels*. Certaines lois promulguées au cours du dernier exercice confèrent aux institutions une capacité sans précédent de communiquer les renseignements personnels des Canadiens à leur insu et sans leur consentement, ce qui met en lumière ce besoin et soulève des questions importantes concernant la surveillance et la transparence. Dans le chapitre 3 du présent rapport, nous revenons sur trois projets de loi relatifs à la surveillance au sujet desquels nous avons témoigné devant le Parlement. Nous y présentons également certaines mesures que nous avons proposées pour protéger la vie privée après la mise en œuvre de ces projets de loi.

Notre rapport, qui met aussi l'accent sur les atteintes à la sécurité des données déclarées au Commissariat ainsi que sur les résultats d'enquêtes et d'une vérification

que nous avons menées, souligne l'importance d'élaborer et d'appliquer des procédures et des mesures de sécurité rigoureuses pour protéger l'information personnelle des Canadiens.

La protection contre les atteintes à la sécurité des données et la prévention des atteintes au droit à la vie privée représentent un défi que l'on ne doit pas ignorer. Par ailleurs, étant donné que les Canadiens doivent fournir des renseignements très sensibles aux ministères et organismes fédéraux, le devoir de diligence du gouvernement revêt une importance cruciale.

De nombreuses institutions ont fait des progrès au chapitre de la protection des renseignements personnels. Il y a toutefois encore grandement matière à amélioration, comme le démontrent les plus de 250 atteintes déclarées au Commissariat au cours de la période couverte par le présent rapport, certaines enquêtes que nous résumons ici et les résultats de notre vérification portant sur les dispositifs de stockage portables.

GROS PLAN SUR LES ATTEINTES À LA SÉCURITÉ DES DONNÉES

Les atteintes à la sécurité des données réduisent le contrôle qu'exercent les gens sur leurs renseignements personnels et minent leur confiance envers les institutions auxquelles ils confient ces renseignements. Dans l'analyse de fond présentée au chapitre 4, nous examinons attentivement certaines atteintes importantes, la façon dont elles sont survenues et les efforts déployés par les institutions responsables pour y réagir et empêcher que des incidents similaires se produisent à l'avenir.

L'exercice écoulé est le premier au cours duquel les lignes directrices révisées du Conseil du Trésor sur les atteintes à la vie privée obligent les institutions à déclarer au Commissariat et au Secrétariat du Conseil du Trésor du Canada les atteintes « substantielles » à la vie privée.

La déclaration obligatoire constitue un important pas en avant. Comme nous l'avons signalé dans nos rapports annuels antérieurs, lorsque la déclaration était volontaire, il était impossible de savoir avec certitude si l'augmentation considérable observée au cours des derniers exercices découlait d'une hausse réelle du nombre d'atteintes à la sécurité des données ou d'une plus grande diligence de la part des institutions en matière de déclaration.

Il s'est écoulé presque un exercice complet depuis l'entrée en vigueur des nouvelles exigences. Nous commençons à avoir une meilleure idée de la situation concernant les atteintes à la sécurité des données au sein de l'administration fédérale, ce qui devrait permettre d'obtenir des données de référence plus précises aux fins de comparaisons à l'avenir. Au cours du dernier exercice, le Commissariat s'est particulièrement attaché à comprendre pourquoi et comment les atteintes surviennent, comment se protéger contre ce type d'incidents et comment atténuer le risque auquel sont exposés les Canadiens en cas

d'incident. Nous poursuivrons nos efforts sur ce front.

Nous avons été témoins de cas où les vulnérabilités d'un réseau et les défaillances technologiques avaient entraîné la communication des renseignements personnels portant sur des Canadiens. Toutefois, d'après notre examen des atteintes à la sécurité des données déclarées en 2014-2015, une communication accidentelle constituait, la cause la plus fréquente des incidents, tout comme au cours des exercises antérieurs. Or, il s'agit d'un risque que des procédures plus rigoureuses permettent souvent d'atténuer. En fait, la communication accidentelle était de loin la cause citée le plus souvent, comptant pour 73 % des incidents déclarés.

Près des trois quarts des atteintes à la sécurité des données auraient pu être évitées si les institutions avaient fait preuve d'une plus grande diligence. Ce fait préoccupant montre que les institutions continuent de subir des atteintes découlant du mauvais acheminement de courrier ou de fenêtres d'enveloppe trop grandes, même si des incidents similaires se répètent depuis des années. Des mesures relativement simples peuvent — et doivent — être prises pour éviter ce type d'atteintes. J'espère que le rapport annuel de 2014-2015 rappellera la nécessité de renforcer la vigilance.

INCIDENCE DES ATTEINTES

Même lorsqu'elles ne sont pas délibérées, les atteintes à la sécurité des données peuvent avoir des conséquences désastreuses.

Dans un exemple cité en détail au chapitre 4, l'Agence du revenu du Canada (ARC) a remis par inadvertance à un journaliste du service journalistique anglophone de la SRC les renseignements personnels associés à plus de 1 000 personnes et entreprises. La SRC a par la suite diffusé un reportage dans lequel elle identifiait plusieurs personnes touchées par l'incident.

Un autre dossier présenté en détail a trait à un incident où Santé Canada a envoyé des lettres à plus de 41 000 personnes de partout au Canada dans des enveloppes laissant voir que les lettres émanaient du Programme d'accès à la marihuana à des fins médicales. Le simple fait qu'une personne s'inscrive à ce type de programme ou qu'elle s'y intéresse constitue manifestement une information très sensible qui ne devrait pas être communiquée sans son consentement explicite.

Dans un autre dossier, le nom des personnes ayant demandé en vertu de la *Loi sur l'accès à l'information* des documents concernant les dépenses d'un ancien ministre des Affaires autochtones et du Développement du Nord a été révélé à des employés du ministère qui n'avaient pas besoin de connaître cette information.

Dans chacun de ces trois dossiers — de même que dans d' autres cas cités dans le présent rapport —, les institutions ont été invitées à améliorer davantage les procédures et à mieux les suivre pour renforcer la protection des renseignements personnels et obtenir les résultats voulus afin de maintenir la confiance du public.

VÉRIFICATION DES DISPOSITIFS DE STOCKAGE PORTABLES

À l'issue de notre vérification menée en 2014-2015, de nombreuses institutions ont également été invitées à améliorer leurs procédures ou à en adopter de nouvelles pour protéger les renseignements personnels qu'elles conservent sur des dispositifs de stockage portables allant de petits disques durs à des dispositifs encore plus petits, par exemple des clés USB. La petite taille et la portabilité de ces dispositifs combinée à leur énorme capacité de stockage de données, en font de précieux outils. Malheureusement, ces caractéristiques font aussi en sorte qu'ils sont facilement perdus ou volés.

Après de nombreuses atteintes à la sécurité des données mettant en cause des dispositifs de stockage portables et touchant des milliers de Canadiens, le Commissariat a amorcé en 2014 une vérification horizontale de la gestion de ces dispositifs au sein des institutions fédérales.

D'après notre vérification, qui est décrite au chapitre 5, les institutions ont accompli des progrès au chapitre de l'atténuation du risque, mais il y a encore matière à amélioration. J'encourage toutes les institutions à examiner nos conclusions en vue de gérer l'utilisation de ces les dispositifs de manière à continuer d'en tirer avantage tout en réduisant le risque d'atteintes au sein de leur organisation. Ce type de mesures pourrait aider le gouvernement fédéral à mieux protéger les données et contribuer par le fait même à réduire le nombre d'atteintes déclarées annuellement.

PLAINTES

Le nombre de plaintes déposées en 2014-2015 auprès du Commissariat concernant le traitement des renseignements personnels des Canadiens par les institutions fédérales est légèrement plus élevé qu'au cours de l'exercice précédent, abstraction faite des nombreuses plaintes émanant de quelques personnes. En ajoutant ces plaintes, on arrive à 3 977 plaintes au total. Si l'on soustrait les plaintes en suspens, il en reste 1 040, ce qui représente une légère hausse annuelle.

À mesure que la demande augmente, nous continuons de chercher des façons d'obtenir des résultats aussi efficacement que possible au bénéfice des parties. Pour utiliser ses ressources limitées de façon plus efficace, le Commissariat a adopté de nombreuses stratégies, notamment le règlement des plaintes par voie de conciliation et de négociation lorsque la situation s'y prête. Je suis heureux d'affirmer que le nombre de plaintes que nous pouvons

résoudre selon notre processus de règlement rapide, qui répond aux besoins des plaignants sans que l'on doive consacrer des ressources considérables à une enquête régulière, continue d'augmenter. Au cours du dernier exercice, 422 plaintes ont été réglées de cette façon.

COMPRENDRE LES PRIORITÉS DES CANADIENS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

En 2014-2015, nous avons déployé de vastes efforts pour déterminer les principaux enjeux relatifs à la vie privée qui touchent le plus les Canadiens afin de renforcer le contrôle global que ceux-ci exercent sur leurs renseignements personnels. Nous souhaitions ainsi établir les priorités stratégiques pour la vie privée qui guideront une partie des travaux du Commissariat au cours des cinq prochaines années.

À cette fin, nous avons organisé partout au Canada des rencontres avec des intervenants — des membres de la société civile, de groupes de défense des consommateurs, des milieux universitaire et juridique, de l'industrie et de l'administration publique, ainsi que nos homologues provinciaux — pour connaître leur opinion sur les enjeux relatifs à la protection de la vie privée qui seront particulièrement importants pour les Canadiens d'ici à 2020. Nous avons aussi consulté la population dans le cadre de groupes de discussion.

Je remercie les intervenants et les citoyens qui ont pris le temps de participer à cette démarche extrêmement utile et de nous faire part de leur opinion.

Le rapport intitulé *Priorités de protection de la vie privée du Commissariat 2015-2020 : Tracer un chemin vers une meilleure protection*, qui est affiché sur notre site Web, résume les propos des individus et des intervenants consultés. Il présente également les quatre priorités retenues en expliquant comment nous avons l'intention d'y donner suite.

Même si nous ne pouvons pas anticiper ou contrôler la majeure partie du travail effectué par le Commissariat, nous bénéficions tout de même d'une certaine latitude pour ce qui est de déterminer les vérifications que nous lançons, le travail d'examen de la conformité que nous entreprenons de notre propre chef, et le type de conseils et d'éducation du public que nous offrons.

ALLER DE L'AVANT AVEC LES NOUVELLES PRIORITÉS STRATÉGIQUES

Les quatre priorités stratégiques retenues nous aideront à orienter et à cibler ces activités discrétionnaires au cours des cinq prochaines années.

L'économie des renseignements personnels

L'importance de l'information dans l'économie et la société actuelles ont a favorisé

la marchandisation des renseignements personnels et l'élaboration de nouveaux modèles opérationnels articulés autour de l'utilisation des mégadonnées, de l'Internet des objets et des technologies mobiles.

Les lois canadiennes sur la protection des renseignements personnels sont fondées sur la capacité des citoyens à exercer un contrôle sur leurs renseignements personnels — et cette capacité repose sur la qualité du consentement. À une époque où l'analytique et les algorithmes permettent de trouver de nouvelles utilisations potentielles de l'information qui n'avaient jamais même pu être conçues ou imaginées, de nombreux participants à notre démarche se demandaient s'il était encore réaliste de solliciter un consentement ponctuel en échange de renseignements personnels.

Notre objectif à ce chapitre consiste à renforcer la protection de la vie privée et la confiance des gens pour leur permettre de participer avec assurance à une économie numérique novatrice.

Le corps comme source d'information

L'information générée par notre corps est à la fois personnelle et unique. Elle peut, à ce titre, être de nature très délicate. De plus en plus de renseignements sur notre corps sont recueillis, numérisés, répertoriés et analysés dans des bases de données biométriques et génétiques, ce qui peut avoir de profondes répercussions sur la vie privée. L'exploitation de cette information à des fins lucratives dans le commerce ou aux fins de la surveillance exercée par le gouvernement pourrait porter atteinte non seulement à la protection de nos renseignements personnels, mais aussi à l'intégrité de notre corps et à notre dignité en tant qu'être humain.

À l'heure actuelle, le gouvernement fédéral élargit l'utilisation qu'il fait du matériel génétique. Des modifications ont été apportées à la *Loi sur l'identification par les empreintes génétiques* en 2014. Le législateur a alors ajouté cinq nouvelles catégories de profil d'identification génétique, entre autres ceux des victimes de crime, des personnes disparues et de leurs parents, ainsi que des personnes qui fournissent volontairement des substances corporelles.

En parallèle, les institutions fédérales utilisent davantage les données biométriques comme identificateur. Ainsi, le projet de loi C59, qui a été adopté en juin 2015, ne limite plus à certains ressortissants étrangers qui entrent au Canada le prélèvement des empreintes digitales. La prise et la conservation des empreintes digitales, d'une image numérisée de l'iris ou de la paume de la main et de photos du visage, en particulier si ces éléments concordent avec d'autres données que le gouvernement possède déjà, peuvent soulever de graves problèmes de protection de la vie privée. Le Commissariat se penchera sur des initiatives dans le cadre desquelles des institutions fédérales souhaitent

utiliser des données concernant les Canadiens ou fournies par ceux-ci pour s'assurer que l'on reconnaît les répercussions des ces activités sur la vie privée et que l'on y donne suite.

Réputation et protection de la vie privée

Internet et la société numérique qu'il a engendrée ont eu une incidence profonde sur la gestion de la réputation personnelle. Lorsque les renseignements personnels sont publiés en ligne dans un contexte donné, il est parfois extrêmement difficile de les éliminer ou d'empêcher qu'ils soient utilisés dans d'autres contextes. Même si les gens évoluent et changent au fil du temps, les renseignements personnels affichés en ligne à leur sujet peuvent revenir les hanter à tout moment.

Dans le contexte du filtrage de sécurité, le gouvernement fédéral fait montre d'un intérêt croissant pour l'utilisation des renseignements personnels accessibles au public, notamment l'information affichée sur les sites de médias sociaux. Cette situation crée un risque de profilage selon lequel les gens pourraient être définis en fonction de leur passé numérique.

Notre objectif consiste à créer un environnement où les gens peuvent utiliser Internet pour explorer leurs champs d'intérêt sans craindre que leur trace numérique n'entraîne un traitement injuste.

Surveillance du gouvernement

Comme on l'explique au chapitre 3, le dernier exercice a été marqué au sein du Parlement par des changements radicaux dans le paysage entourant la sécurité nationale. Avec l'adoption du projet de loi C51, *Loi antiterroriste de 2015* — qui englobe la *Loi sur la communication d'information ayant trait à la sécurité du Canada* —, les Canadiens peuvent s'attendre à ce qu'une quantité croissante de leurs renseignements personnels soient communiquée à un plus large éventail d'institutions gouvernementales aux fins générales de contrer les « activités qui portent atteinte à la sécurité du Canada ».

En résumé, cette loi permet à toutes les institutions fédérales du Canada de communiquer toute information qu'elles ont recueillie concernant des Canadiens aux 17 ministères et organismes fédéraux dont le mandat, en tout ou en partie, est en lien avec la sécurité nationale pour autant que l'information « se rapporte » au mandat de l'institution destinataire à cet égard.

Comme je l'ai expliqué en détail au Parlement, le prix à payer sur le plan de la protection de la vie privée pour atteindre l'objectif de la loi, à savoir permettre la communication d'information pour détecter les menaces, me semble beaucoup trop élevé. Le législateur a ouvert la voie à une collecte et une communication disproportionnées des renseignements personnels de citoyens

ordinaires respectueux de la loi. Cet état de choses laisse entrevoir un profilage et un recours à l'analytique de mégadonnées visant tous les Canadiens.

Entre autres préoccupations, le seuil établi pour autoriser la communication d'information — obligation qu'elle « se rapporte » à la sécurité nationale — met la barre beaucoup trop bas. J'ai recommandé de modifier le projet de loi de manière à autoriser plutôt la communication si elle est « nécessaire » ou « proportionnelle » au mandat de l'institution destinataire. De plus, aucune obligation claire concernant la conservation et la destruction des renseignements personnels n'est imposée aux organisations. Il s'agit d'une lacune flagrante.

Enfin, la communication supplémentaire de renseignements personnels autorisée par la législation n'est pas accompagnée d'un renforcement correspondant de la surveillance. En fait, seulement trois des 17 ministères et organismes autorisés à recevoir de l'information aux fins de la sécurité nationale en vertu de la loi, doivent faire l'objet d'une surveillance ou un examen indépendant effectué par un organisme distinct.

À court et à moyen terme, nous examinerons la façon dont sera mise en œuvre la législation sur la sécurité nationale, comme le projet de loi C51, et nous ferons rapport sur le sujet. Nous avons l'intention d'exercer nos pouvoirs d'examen et d'enquête pour nous pencher sur les pratiques de collecte, d'utilisation et de communication des ministères et organismes exerçant des activités de surveillance, afin de nous assurer qu'elles sont conformes à la *Loi sur la protection des renseignements personnels*. Nous présenterons nos conclusions aux parlementaires et à la population et nous recommanderons des mesures en vue d'améliorer les politiques ou la législation selon les besoins.

REGARD EN AVANT

La majeure partie du présent rapport porte forcément sur l'examen de nos activités au cours de l'exercice écoulé, mais nous devons aussi nous tourner vers l'avenir.

Nous avons adopté des approches stratégiques pour traduire nos priorités pour la protection de la vie privée en mesures concrètes. À cette fin, nous préconiserons des moyens technologiques novateurs de protéger la vie privée; nous favoriserons une imputabilité accrue et une meilleure gouvernance de la protection des renseignements personnels; nous collaborerons dans la mesure du possible avec nos partenaires chargés de la surveillance de la protection de la vie privée; nous chercherons de nouvelles façons de joindre les citoyens et de les renseigner sur la protection de la vie privée; et nous nous attacherons à aider les groupes particulièrement vulnérables aux atteintes à la vie privée (notamment les jeunes et les personnes âgées).

Nous avons fixé ces priorités en vue d'atteindre l'objectif d'amener les Canadiens à exercer un meilleur contrôle sur leurs renseignements personnels, tout en accomplissant toutes les tâches qui nous sont confiées. J'ai le privilège de participer à cette demarche avec le soutien et les conseils d'une équipe de personnes talentueuses et compétentes qui unissent leurs efforts pour protéger le droit des Canadiens à la vie privée.

La protection de la vie privée en chiffres

Demandes de renseignements reçues au titre de la *Loi sur la protection des renseignements personnels*	**1 461**
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées et actives	**1 040**
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées et en suspens[1]	**2 937**
Plaintes en vertu de la Loi sur la protection des renseignements personnels fermées à l'issue d'un processus de règlement rapide	**422**
Plaintes en vertu de la Loi sur la protection des renseignements personnels fermées à l'issue d'une enquête régulière	**1 485**
Évaluations des facteurs relatifs à la vie privée examinées — risque élevé	**51**
Évaluations des facteurs relatifs à la vie privée examinées — risque faible	**22**
Vérifications dans le secteur public menées à bien	**1**
Communication de renseignements par des organisations fédérales pour des raisons d'intérêt public	**266**
Lois concernant le secteur public fédéral examinées sous l'angle de leurs répercussions sur la vie privée	**14**
Politiques ou initiatives du secteur public examinées sous l'angle de leurs répercussions sur la vie privée	**38**
Comparutions devant des comités parlementaires sur des questions touchant le secteur public	**12**

1 Les plaintes en suspens ont été déposées par quelques personnes seulement.

Mémoires officiels présentés sur des questions touchant le secteur public	**11**
Autres contacts avec des parlementaires ou leur personnel (par exemple, correspondance avec les bureaux de députés ou de sénateurs) sur des questions touchant le secteur public	**19**
Discours prononcés et présentations données*	**99**
Visites sur le site Web principal*	**2 448 066**
Visites dans les blogues*	**1 103 262**
Visites sur la chaîne YouTube*	**39 812**
Tweets envoyés*	**743**
Personnes qui suivaient le Commissariat sur Twitter au 31 mars 2015 *	**9 426**
Publications diffusées*	**8 229**
Communiqués et annonces publiés*	**33**

* *Activités qui ne se limitent pas à des questions touchant le secteur public, mais qui reflètent l'ensemble du travail accompli par le Commissariat entre le 1er avril 2014 et le 31 mars 2015*

Devant le Parlement : pleins feux sur la surveillance

Comme le commissaire l'a mentionné dans son message, l'exercice écoulé a été marqué par de grandes transformations au chapitre de la surveillance exercée par le gouvernement. Les répercussions éventuelles de ces changements sur la vie privée des Canadiens revêtent une importance cruciale pour le Commissariat.

Dans le cadre de l'établissement de nos priorités, il a été question à maintes reprises, au cours de nos consultations auprès des intervenants et des Canadiens participant aux groupes de discussion, de la capacité et du pouvoir toujours plus grands des organismes gouvernementaux de recueillir et de communiquer les renseignements personnels des Canadiens. Les préoccupations qu'ils ont formulées, de même que nos propres préoccupations, nous ont incités à faire de la surveillance du gouvernement l'une de nos quatre priorités stratégiques[2].

Certes, personne ne niera la nécessité d'assurer la sécurité du public, que la menace soit le terrorisme ou le risque que nos enfants soient victimes d'intimidation ou de harcèlement en ligne. Les Canadiens veulent être en sécurité et se sentir protégés, mais pas au détriment de leur vie privée. Bref, ils veulent à la fois la sécurité et la protection de leur vie privée. Soulignons que les participants aux groupes de discussion de 2014 voyaient généralement d'un bon œil la surveillance exercée par le gouvernement pour assurer la sécurité nationale et prévenir les actes criminels. Toutefois, lorsqu'on leur demandait leur opinion sur une surveillance qui viserait leurs propres communications, nombre d'entre eux n'aimaient pas l'idée que l'on établisse leur profil à leur insu et craignaient que cette pratique n'entraîne une violation des droits et libertés fondamentaux.

Plusieurs initiatives législatives ont attiré l'attention du Commissariat en 2014-2015. Celui-ci a par ailleurs fait part de ses préoccupations aux parlementaires en déposant des mémoires et en témoignant devant des comités de la Chambre des communes et du Sénat.

2 https://www.priv.gc.ca/information/pub/pp_2015_f.asp

EXAMEN DE LA SURVEILLANCE EXERCÉE PAR LE GOUVERNEMENT

La période couverte par le présent rapport a été marquée par trois projets de loi particuliers qui s'entrecroisent du fait qu'ils renforcent la capacité du gouvernement à recueillir, à utiliser et à communiquer des renseignements personnels concernant des Canadiens sans le consentement de ces derniers.

****

Projet de loi C-51

Le projet de loi C-51, *Loi antiterroriste de 2015*, a été déposé au Parlement en janvier 2015. Il englobe la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), qui confère à toutes les institutions fédérales le pouvoir discrétionnaire de communiquer des renseignements personnels recueillis auprès des Canadiens aux 17 ministères ou organismes fédéraux expressément mentionnés dont le mandat, en tout ou en partie, est en lien avec des « activités qui portent atteinte à la sécurité du Canada » — dans la mesure où l'information se rapporte au mandat de l'institution destinataire à cet égard.

Dans une résolution conjointe soumise avant le dépôt du projet de loi C-51, le commissaire fédéral et ses homologues provinciaux et territoriaux exhortaient le gouvernement fédéral à adopter une démarche fondée sur les données factuelles avant d'instaurer de nouvelles mesures législatives accordant des pouvoirs supplémentaires aux organismes de sécurité nationale.

Après le dépôt du projet de loi C-51, le Commissariat a exprimé dans des mémoires au Parlement ses nombreuses préoccupations concernant la LCISC[3], et nous avons suivi avec grand intérêt le débat public animé et soutenu concernant ce projet de loi.

La LCISC, entrée en vigueur en août 2015, confère à 17 institutions gouvernementales dont le mandat comprend la sécurité nationale des pouvoirs pratiquement illimités pour surveiller les Canadiens ordinaires et établir leur profil grâce à l'analyse de mégadonnées, dans le but de repérer parmi eux ceux qui constituent une menace pour la sécurité.

Parmi les autres changements qu'il a proposés, le Commissariat a recommandé que le projet de loi autorise la communication de renseignements personnels par les institutions fédérales uniquement si elle est « nécessaire ou proportionnelle » au mandat conféré par la loi à l'institution concernant les « activités qui portent atteinte à la sécurité du Canada » et non simplement si la communication d'information « se rapporte » au mandat de l'institution destinataire. De plus, au lieu d'imposer au ministère qui communique

3 https://www.priv.gc.ca/parl/2015/parl_sub_150305_f.asp
https://www.priv.gc.ca/parl/2015/parl_sub_150416_f.asp
https://www.priv.gc.ca/parl/2015/parl_20150423_f.asp

Autres témoignages devant des comités et mémoires déposés au Parlement sur des questions touchant le secteur public en 2014-2015

Outre les questions traitées en détail dans le présent rapport, le Commissariat a donné des avis aux parlementaires dans de nombreux autres dossiers touchant le secteur public :

- **Comparution devant le Comité sénatorial de la sécurité nationale et de la défense concernant les mesures de sécurité à la frontière de l'Agence des services frontaliers du Canada (ASFC)** — le 28 avril 2014
- **Projet de loi C-31, la *Loi nº 1 sur le plan d'action économique de 2014* — Mémoire présenté au Comité sénatorial permanent des finances nationales** — le 13 mai 2014
- **Projet de loi C-247, Loi élargissant le mandat de Service Canada en cas de décès d'un citoyen canadien ou d'un résident canadien — Mémoire présenté au Comité permanent des ressources humaines, du développement des compétences, du développement social et de la condition des personnes handicapées (HUMA)** — le 29 octobre 2014
- **Comparution devant le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie concernant la Section 17 du projet de loi C-43, Loi nº 2 sur le plan d'action économique de 2014, Modification de la *Loi sur l'identification par les empreintes génétiques*** — le 5 novembre 2014
- **Projet de loi C-32, *Loi édictant la Charte canadienne des droits des victimes et modifiant certaines lois*, aussi connu comme la *Charte canadienne des droits des victimes* — Mémoire présenté au Comité permanent de la justice et des droits de la personne (JUST)** — le 13 novembre 2014
- **Comparution devant le Comité permanent des Finances de la Chambre des communes sur la Partie IV du projet de loi C-43 (*Loi nº 2* sur le plan d'action économique de 2014)** — le 24 novembre 2014
- **Projet de loi C-520, *Loi sur l'impartialité politique des bureaux des agents* — Mémoire présenté au Comité sénatorial permanent des finances nationales** — le 28 janvier 2015
- **Comparution devant le Comité permanent de la justice et des droits de la personne (JUST) de la Chambre des communes au sujet du Projet de loi C-26, *Loi sur les peines plus sévères pour les prédateurs d'enfants*** — le 16 février 2015
- **Comparution devant le Comité permanent des Finances de la Chambre des communes sur le financement du terrorisme au Canada et à l'étranger** — le 31 mars 2015

l'information le fardeau de déterminer quelle information pourrait être nécessaire aux fins de la sécurité nationale, le projet de loi devrait obliger de façon explicite le ministère destinataire — qui aurait vraisemblablement les compétences voulues — à déterminer si l'information est effectivement nécessaire pour des fins liées à son mandat de sécurité et, dans le cas contraire, il devrait exiger que ce ministère détruise l'information sans attendre.

Notre mémoire soulevait également les préoccupations suivantes concernant le projet de loi :

- il n'établit aucune limite claire quant à la période de conservation de l'information;
- il n'exige pas que la communication d'information fasse l'objet d'ententes écrites;
- il n'offre aucun recours judiciaire aux personnes touchées par une collecte, une utilisation ou une communication inappropriées de leurs renseignements personnels.

Ces préoccupations ont été accentuées par l'absence de dispositions prévoyant une forme quelconque de surveillance ou d'examen de la communication, de la collecte, de l'utilisation et de la conservation de renseignements personnels autorisées par le projet de loi C-51. En fait, seuls trois des 17 ministères et organismes autorisés à recevoir l'information doivent faire l'objet d'une surveillance ou d'un examen effectué par un organisme indépendant distinct. Un examen indépendant est d'autant plus essentiel que la communication d'information se fera souvent sous le sceau du secret.

Projet de loi C-13

En novembre 2014, dans un mémoire présenté au Comité sénatorial permanent des affaires juridiques et constitutionnelles et au cours de sa comparution devant ce comité, le commissaire a exposé en détail de nombreuses préoccupations suscitées par le projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*. Le Commissariat s'est déclaré favorable à l'objectif premier du projet de loi, plus précisément les articles créant de nouvelles infractions criminelles pour combattre la cyberintimidation et d'autres formes d'exploitation et de harcèlement en ligne — des activités qui présentent manifestement toutes de graves risques d'atteinte à la dignité individuelle et à la vie privée de tous les citoyens qui utilisent les réseaux sociaux et les communications en ligne.

Par ailleurs, le pouvoir de recueillir les renseignements personnels des Canadiens — élargi en vertu du projet de loi — va toutefois trop loin en abaissant le seuil à partir duquel les autorités peuvent obtenir une ordonnance de production obligeant un fournisseur de services Internet à transmettre

de l'information sur ses abonnés. En pareil cas, il suffit qu'un fonctionnaire public *soupçonne* une personne de s'adonner à une activité illégale pour fouiller dans sa vie numérique, par opposition au seuil plus élevé prévu par la loi exigeant des « motifs raisonnables de croire » qu'une perquisition ferait la preuve qu'un crime particulier a été commis.

À cet égard, la définition trop large du terme « fonctionnaire public » énoncée dans le projet de loi C-13 pourrait donner lieu à la collecte de renseignements personnels à des fins très variées. Autrement dit, selon le seuil abaissé, le projet de loi autoriserait non seulement les policiers, mais aussi les préfets, les agents des pêches et les maires, entre autres, à avoir accès en toute légitimité aux renseignements personnels des Canadiens.

En outre, dans son témoignage devant le Comité en novembre 2014, le commissaire a soulevé des préoccupations concernant l'absence d'un mécanisme de reddition de comptes « permettant aux Canadiens de tenir le gouvernement responsable de l'exercice de ces nouveaux pouvoirs importants et lorsqu'il effectue des demandes sans mandat ». Le commissaire a également fait part de son inquiétude concernant la clause d'immunité du projet de loi C-13, qui vise à protéger contre d'éventuelles poursuites les personnes qui communiquent de leur plein gré des renseignements personnels à la suite de demandes d'accès sans mandat émanant du gouvernement. Il a souligné que cette clause était ambigüe, car elle était formulée quelques mois seulement après l'arrêt unanime de la Cour suprême du Canada dans *R. c. Spencer*, qui limitait clairement les perquisitions sans mandat aux situations où il y a des circonstances contraignantes, une loi qui n'a rien d'abusif ou de l'information qui ne fait pas l'objet d'une attente raisonnable en matière de vie privée.

Le projet de loi C-13 a été adopté sans amendement en décembre 2014.

Projet de loi C-44

Le projet de loi C-44, *Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et d'autres lois*, a été déposé à la Chambre des communes en octobre 2014. Il proposait d'autoriser explicitement le Service canadien du renseignement de sécurité (SCRS) à exercer ses activités à l'extérieur du Canada. Il n'est pas inconcevable — en fait, il semble probable — que cette mesure accroîtrait la communication d'information avec des partenaires étrangers.

Comme nous l'avons vu, la communication d'information avec des gouvernements étrangers peut entraîner de graves atteintes aux droits de la personne, voire des cas de torture — le cas bien connu de Maher Arar, citoyen canadien innocent détenu et torturé en Syrie pendant près d'un an en constitue un exemple. En 2006, la commission d'enquête O'Connor a conclu que les représentants

canadiens avaient fort probablement fourni aux autorités américaines des renseignements inexacts sur M. Arar, ce qui a entraîné son expulsion en Syrie.

Dans des mémoires présentés au Comité sénatorial permanent de la sécurité nationale et de la défense et au Comité permanent de la sécurité publique et nationale, le commissaire a recommandé d'ajouter au projet de loi des dispositions empêchant toute communication d'information par le SCRS qui entraînerait une violation des obligations internationales du Canada, notamment à titre de signataire de la *Convention des Nations Unies contre la torture et autres peines ou traitements cruels, inhumains ou dégradants*.

Le projet de loi C-44 a été adopté sans amendement et a reçu la sanction royale en avril 2015.

****

Dans l'ensemble, tous les projets de loi analysés ici sont reliés par un fil conducteur : chacun élargira le pouvoir du gouvernement et de ses agents de recueillir, d'utiliser et de communiquer les renseignements personnels des Canadiens à leur insu et sans leur consentement ainsi que sans augmentation proportionnée de la surveillance ou de l'examen indépendant afin de s'assurer que ces pouvoirs ne sont pas utilisés à mauvais escient ou de façon abusive.

Ensemble, ces initiatives ont créé ce que l'on ne peut décrire que comme un « changement radical » pour le droit à la vie privée au Canada. Au cours des mois et des années à venir, le Commissariat continuera tout particulièrement à s'assurer que les pouvoirs conférés au gouvernement en vertu de ces nouvelles lois sont exercés dans le respect de la vie privée.

Dans la foulée de l'établissement de nos priorités, nous nous sommes fixé comme objectif de contribuer à l'adoption et à la mise en œuvre de lois et d'autres mesures qui assurent de façon manifeste la sécurité nationale et la protection de la vie privée.

Déjà, en ce qui concerne les dispositions du projet de loi C-13 portant sur l'accès légitime, nous avons collaboré avec d'autres intervenants pour élaborer à l'intention du secteur privé des lignes directrices en vue de l'établissement de normes régissant la production de rapports de transparence et de rapports redditionnels concernant la communication de renseignements personnels par les entreprises aux organismes chargés de l'application de la loi. Le Commissariat a également demandé aux institutions fédérales de commencer à publier elles-mêmes des rapports de transparence relativement aux demandes de renseignements sur des clients qu'elles adressent aux organisations du secteur privé.

L'an dernier, le Commissariat a procédé à un examen de la pratique de la Gendarmerie royale du Canada (GRC) consistant à recueillir sans mandat des renseignements sur les abonnées auprès des fournisseurs de services de télécommunications. À l'issue de cet examen, il a recommndé à la GRC de mettre en place un mécanisme de surveillance et de production de rapports concernant la collecte de renseignements en pareil cas. La mise en œuvre de cette recommandation progresse plus lentement que prévu. Comme le nouveau gouvernement s'est engagé à promouvoir l'ouverture et la transparence au sein des institutions fédérales, nous espérons qu'il prendra des mesures à cet égard.

REGARD EN AVANT

À court terme, à la lumière de l'examen des évaluations des facteurs relatifs à la vie privée, nous formulerons des recommandations dans le but d'atténuer les risques d'atteinte à la vie privée associés à la *Loi antiterroriste de 2015* récemment adoptée.

À l'avenir, nous examinerons la façon dont sera mise en œuvre la législation sur la sécurité nationale et nous ferons rapport sur le sujet. Nous exercerons nos pouvoirs d'examen et d'enquête pour nous pencher sur les pratiques de collecte, d'utilisation et de communication des institutions fédérales exerçant des activités de surveillance, afin de nous assurer qu'elles se conforment à la *Loi sur la protection des renseignements personnels*. Nous présenterons nos conclusions aux parlementaires et à la population et nous recommanderons des mesures en vue d'améliorer les politiques ou la législation selon les besoins.

Atteintes à la sécurité des données : renforcement des incitatifs pour mieux gérer les risques, prévenir la perte de données et maintenir la confiance des Canadiens

Avec les nouveaux moyens à leur disposition et leurs nouveaux pouvoirs de collecte de renseignements personnels, les institutions fédérales détiennent de plus en plus de renseignements nous concernant — des données stockées à divers endroits et sur divers supports, qui sont utilisées, communiquées et transmises dans toute une gamme de formats et à des fins de plus en plus variées.

Chacune de ces transactions de données, et d'innombrables autres, ajoutent un niveau de risque supplémentaire de communication des renseignements personnels, que ce soit de façon accidentelle ou délibérée ou en raison d'une défaillance technique.

Les renseignements personnels des Canadiens sont régulièrement recueillis et utilisés par les institutions fédérales, par nécessité de se conformer à la loi, et non par choix personnel. Bien souvent, ces renseignements sont de nature très délicate. C'est pourquoi la diligence qu'exercent les institutions doit satisfaire aux normes les plus strictes. Il n'est sans doute pas raisonnable de s'attendre à la perfection absolue à cet égard, mais les institutions doivent élaborer, appliquer et suivre des procédures rigoureuses pour assurer une protection des renseignements personnels répondant aux attentes des Canadiens. Toute lacune à cet égard risque de miner la confiance du public.

De nombreux participants à une série de groupes de discussions organisés par le Commissariat à l'automne 2014 ont cité les atteintes à la sécurité des données pour souligner leurs préoccupations concernant la capacité du gouvernement à traiter comme il se doit leurs renseignements personnels.

Des préoccupations similaires sont ressorties d'un sondage mené auprès de quelque 1 500 Canadiens pour le compte du Commissariat à l'automne dernier : près du tiers des répondants ont indiqué ne pas avoir confiance dans la capacité du gouvernement à s'assurer que leurs renseignements ne seraient pas perdus, volés ou utilisés à mauvais escient.

2014-2015 : DÉBUT DE LA DÉCLARATION OBLIGATOIRE

Au cours du dernier exercice, les institutions fédérales ont déclaré au Commissariat 256 atteintes à la sécurité des données. Il s'agit d'une hausse par rapport aux 228 atteintes déclarées au cours de l'exercice précédent — lesquelles étaient deux fois plus nombreuses comparativement à l'exercice antérieur.

Comme le commissaire l'a mentionné dans son message, l'exercice 2014-2015 constituait le premier exercice où les institutions étaient tenues de déclarer les atteintes à la sécurité des données, puisque le régime en place auparavant reposait sur la déclaration volontaire. Cette nouvelle exigence devrait permettre d'établir un point de référence plus clair aux fins de comparaison à l'avenir.

En vertu de la version mise à jour de la *Directive sur les pratiques relatives à la vie privée* du président du Conseil du Trésor, qui est entrée en vigueur en mai 2014, toutes les atteintes substantielles à la vie privée doivent

La déclaration obligatoire des atteintes à la vie privée s'étend au secteur privé

Un peu plus d'un an après l'entrée en vigueur de la directive du président du Conseil du Trésor sur la déclaration obligatoire des atteintes substantielles à la vie privée mettant en cause les institutions fédérales, le projet de loi S-4, *Loi sur la protection des renseignements personnels numériques*, a reçu la sanction royale. La nouvelle loi a modifié la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), entre autres en exigeant que les organisations avisent les personnes touchées par des atteintes à la sécurité « présentant un risque réel de préjudice grave » et qu'elles les déclarent ces atteintes au Commissariat.

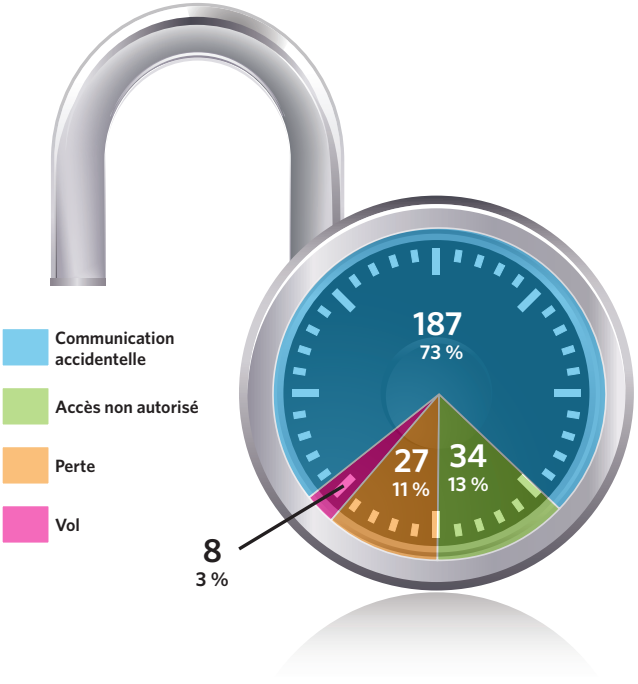
En outre, une organisation devra aviser toute autre organisation ou institution gouvernementale si elle estime que l'autre organisme pourrait réduire le risque de préjudice. Par exemple, un détaillant pourrait envoyer un avis à une banque émettrice de cartes de crédit ou à un organisme chargé de l'application de la loi.

Au moment de la rédaction du présent rapport, le gouvernement fédéral élaborait le règlement appelé à préciser les nouvelles exigences. L'obligation de déclarer les atteintes à la vie privée entrera en vigueur uniquement lorsque le règlement s'appliquera.

être déclarées au Commissariat et au Secrétariat du Conseil du Trésor du Canada. La directive donne une orientation pour aider à établir la distinction entre une « atteinte substantielle » et une atteinte ayant moins de répercussions et présentant un risque qui peut être géré à l'interne, sans déclaration officielle. En bref, les atteintes substantielles à la vie privée dévoilent des renseignements personnels de nature délicate et pourraient raisonnablement causer des dommages ou des préjudices graves à un ou à de nombreux individus.

L'obligation de déclarer les atteintes substantielles à la vie privée constitue un pas en avant, mais on ne peut affirmer avec certitude que l'augmentation du nombre d'atteintes déclarées en 2014-2015 est entièrement attribuable à la directive révisée. Il se peut tout simplement que les institutions fassent preuve d'une plus grande diligence à cet égard. Nous avons constaté que 10 % des institutions assujetties à la *Loi sur la protection des renseignements personnels* avaient déclaré une atteinte au cours du dernier exercice, ce qui correspond au taux de déclaration volontaire enregistré au cours du cycle précédent.

Ventilation des atteintes à la sécurité des données



Lorsqu'une atteinte substantielle est déclarée au Commissariat, le commissaire peut, s'il a des motifs raisonnables de le faire, prendre l'initiative d'une enquête pour déterminer ce qui s'est passé et pour quelles raisons, et recommander des améliorations aux pratiques de gestion des renseignements personnels pour éviter tout incident similaire à l'avenir.

Comme l'illustrent les incidents résumés ci-après, les institutions peuvent généralement éviter les atteintes à la sécurité des données, mais seulement si elles accordent la priorité à la sécurité des renseignements personnels des Canadiens et qu'elles l'intègrent à leur culture organisationnelle. Il est tout aussi important que les institutions soient préparées à réagir efficacement et de façon appropriée en cas d'atteinte, de façon à atténuer les répercussions sur les personnes touchées.

ATTEINTES À LA SÉCURITÉ DES DONNÉES À L'AGENCE DU REVENU DU CANADA

En vertu de son mandat, l'Agence du revenu du Canada (ARC) traite une grande quantité de renseignements personnels de nature délicate concernant les Canadiens. En 2014-2015, elle a déclaré au Commissariat plusieurs atteintes attribuables à divers facteurs, dont la communication accidentelle, le vol et l'accès non autorisé. On trouvera ci-après un exemple d'incident pour chaque catégorie.

Communication accidentelle de renseignements sur des contribuables au service journalistique anglophone de la Société Radio-Canada

En novembre 2014, l'ARC a avisé le Commissariat que les renseignements personnels de plus de 1 000 personnes et entreprises avaient été transmis par inadvertance à un journaliste du service journalistique anglophone de la Société Radio-Canada (SRC). La SRC a diffusé un reportage en se fondant sur l'information reçue, entre autres le nom de certaines personnes touchées ainsi que des détails d'un crédit d'impôt particulier qu'elles avaient demandé. Neuf personnes ont déposé une plainte contre l'ARC auprès du Commissariat. Plusieurs autres se sont également plaintes du fait que SRC avait communiqué leurs renseignements personnels sans leur consentement.

Notre enquête a confirmé que les renseignements transmis à la SRC étaient en fait destinés au Service canadien d'appui aux tribunaux administratifs (SCATA). Ils ont été livrés aux bureaux de la SRC par suite d'un mélange dans les lettres d'accompagnement. Des employés du bureau de l'accès à l'information et de la protection des renseignements personnels (BAIPRP) de l'Agence avaient constaté l'erreur initiale et l'avaient corrigée la veille, mais d'autres employés qui n'étaient pas au courant de l'incident ont répété l'erreur en l'absence de leurs collègues qui avaient remédié à la situation.

Cette atteinte aurait pu être évitée si l'ARC avait mis en place des procédures obligeant le personnel de son BAIPRP à consigner les demandes de renseignements et à suivre l'état d'avancement de leur traitement. À l'issue de notre enquête, nous avons conclu que les plaintes contre l'ARC étaient fondées. En ce qui concerne les plaintes déposées contre la SRC, nous avons conclu qu'elles étaient non fondées car la *Loi sur la protection des renseignements personnels* ne s'applique pas aux renseignements personnels recueillis, utilisés ou communiqués par la SRC à des fins journalistiques, artistiques ou littéraires.

Colmatage de la faille Heartbleed

L'intrusion dans les réseaux constitue une menace constante à la sécurité des renseignements personnels stockés dans les bases de données publiques et privées. Une gestion du risque appropriée consiste notamment à être prêt à réagir rapidement en cas d'atteinte à la sécurité des données. En avril 2014, en tirant parti de la faille Heartbleed (faille de sécurité touchant certains logiciels qu'utilisent des sites Web « sécurisés » pour crypter des noms d'utilisateur, des mots de passe et des renseignements financiers), un intrus a eu accès aux numéros d'assurance sociale et à d'autres renseignements personnels de quelque 900 contribuables. L'ARC a été victime de cette intrusion, mais elle a pu réagir rapidement et fermement.

L'Agence a notamment mis à l'arrêt son système de dépôt électronique à l'approche de la date limite de dépôt des déclarations d'impôt sur le revenu, renforcé la surveillance de ses systèmes informatiques pour détecter les intrusions, envoyé une lettre recommandée à chaque personne touchée par l'intrusion et établi une ligne sans frais expressément pour les victimes de l'intrusion. Elle a également offert aux personnes touchées l'accès à des services de protection du crédit et marqué leur compte à l'ARC afin que l'on puisse y détecter toute activité non autorisée. L'Agence a de plus indiqué à Emploi et Développement social Canada les numéros d'assurance sociale compromis pour que ce ministère puisse surveiller lui aussi les comptes en question.

Accès non autorisé aux dossiers de contribuables

En 2014-2015, l'ARC a déclaré deux cas d'accès non autorisé survenus en 2012. Ces deux incidents mettent en évidence le risque associé au fait qu'une large gamme d'employés avaient accès aux renseignements personnels des contribuables.

En août 2012, l'Agence a constaté qu'un employé de son Bureau des services fiscaux de London-Windsor avait consulté les comptes de 170 personnes. Quelques mois plus tard, soit en janvier 2013, un employé du même bureau a consulté 169 comptes. Les comptes des contribuables touchés contenaient une grande quantité de renseignements personnels de nature délicate — nom, adresse, numéro d'assurance sociale, renseignements sur le revenu, renseignements bancaires, etc. Dans les deux cas, les données de certains comptes avaient été modifiées.

L'ARC a avisé les personnes touchées de l'atteinte en précisant qu'elles pouvaient porter plainte auprès du Commissariat. Elle a pris des mesures disciplinaires contre les employés en cause dans les deux incidents et donné à son personnel une

formation supplémentaire sur la protection des renseignements personnels. Notre vérification de l'ARC effectuée en 2013 nous a permis de constater la nécessité pour l'Agence de renforcer son système national de piste de vérification en ligne et son processus de journalisation pour mieux se protéger contre l'accès non autorisé aux renseignements personnels des contribuables. L'ARC a indiqué qu'elle prenait des mesures en réponse à cette recommandation.

Dans les exemples tirés du dernier exercice, l'ARC a déployé des efforts pour nous informer des incidents et montré qu'elle prend ces questions au sérieux. Dans certains cas, comme dans l'incident de la faille Heartbleed, l'Agence a rapidement pris des mesures énergiques pour protéger les renseignements personnels. En revanche, dans d'autres cas cités en exemple, les problèmes constatés dans le passé se sont répétés en raison de processus inadéquats que l'Agence s'est engagée à corriger et sur lesquels nous effectuerons un suivi.

Comme nous l'avons mentionné, le Commissariat a effectué en 2013 une vérification de l'ARC qui portait principalement sur les mécanismes de contrôle de l'accès aux renseignements personnels. Nous avions alors formulé 13 recommandations touchant de nombreux aspects, entre autres la déclaration des atteintes à la vie privée, la surveillance des droits d'accès des employés, les évaluations de la menace et du risque pour les systèmes de technologie de l'information et l'évaluation des facteurs relatifs à la vie privée pour les nouveaux programmes entraînant des modifications à la gestion des renseignements personnels.

L'ARC était d'accord avec toutes nos recommandations et nous a présenté un plan faisant état des mesures correctives prévues. Nous ferons à l'hiver 2016 un suivi des progrès réalisés par l'Agence à l'égard de ses engagements et poursuivrons nos échanges avec elle concernant ses pratiques de traitement des renseignements personnels.

ATTEINTES CAUSÉES PAR L'UTILISATION D'ENVELOPPES À FENÊTRE

Santé Canada — Programme d'accès à la marihuana à des fins médicales

En 2013, Santé Canada a fait parvenir à plus de 41 000 personnes partout au pays une lettre les informant de modifications prévues au Programme d'accès à la marihuana à des fins médicales (PAMFM). Comme ses enveloppes préimprimées n'étaient pas compatibles avec l'équipement automatisé utilisé par Postes Canada, on a envoyé les lettres dans des enveloppes à fenêtre qui révélaient non seulement le nom et l'adresse du destinataire, mais aussi ceux de l'expéditeur, en l'occurrence le PAMFM.

Santé Canada n'a pas déclaré cette atteinte à la sécurité des données, mais il a affiché sur son

site Web un avis indiquant qu'« en raison d'une erreur administrative, l'étiquette des enveloppes indiquait qu'elles avaient été envoyées par le Programme ». Le commissaire a jugé qu'il avait des motifs raisonnables de prendre l'initiative d'une enquête sur le ministère — une enquête englobant les 339 plaintes déposées par les destinataires des lettres.

Les plaignants alléguaient que Santé Canada avait communiqué leurs renseignements personnels sans leur consentement et faisaient état des nombreuses conséquences graves susceptibles d'en découler, notamment l'atteinte à leur réputation et la crainte de perdre leur gagne-pain si leur employeur apprenait qu'ils consommaient de la marihuana à des fins médicales.

Notre enquête nous a amenés à conclure que Santé Canada avait communiqué des renseignements personnels de nature délicate sans le consentement des personnes visées, bien que le ministère prétende le contraire et qu'il s'agisse d'un incident survenu par inadvertance. Depuis l'incident, le ministère a mis en place des procédures strictes pour les envois postaux afin de protéger les renseignements personnels de ses clients.

Service des poursuites pénales du Canada — Communication des numéros d'assurance sociale indiqués sur des relevés d'impôt

Des enveloppes à fenêtre sont également à l'origine de la communication non autorisée de renseignements personnels par le Service des poursuites pénales du Canada (SPPC), mais cette institution a réagi à l'atteinte de façon très dynamique.

En février 2015, le SPPC a indiqué avoir envoyé par la poste à 65 employés des relevés d'impôt dans des enveloppes à fenêtre trop grandes, si bien que l'on pouvait voir le numéro d'assurance sociale des destinataires dans la fenêtre. Dès qu'il a constaté l'erreur, le Service a informé verbalement les personnes touchées. Il leur a ensuite fait parvenir une lettre expliquant la nature de l'atteinte, leur offrant un service de protection pour surveiller l'activité dans leur dossier de crédit afin de détecter toute fraude ou tout vol d'identité éventuel pendant un an et leur conseillant de surveiller leurs relevés financiers afin d'y détecter doute activité douteuse. La lettre mentionnait également aux employés qu'ils pouvaient porter plainte auprès du Commissariat.

Le SPPC a été en mesure de vérifier que toutes les enveloppes, à l'exception de deux, avaient été livrées aux destinataires. Pour l'une des deux enveloppes non distribuées, l'adresse était celle d'un immeuble démoli; dans l'autre cas,

l'enveloppe n'a pas été retrouvée. Le SPPC a indiqué qu'en plus de mettre fin à l'utilisation des enveloppes à fenêtre pour les relevés d'impôt, il indiquerait une adresse de retour pour que le courrier non distribuable puisse lui être renvoyé.

CITOYENNETÉ ET IMMIGRATION CANADA — ATTEINTE À LA SÉCURITÉ DES DONNÉES TRANSFRONTIÈRES

Dans le cadre de leur coopération sur les questions de sécurité, le Canada et les États-Unis ont mis en place un système informatique leur permettant d'échanger de l'information sur les ressortissants d'autres pays qui demandent un visa ou un permis de voyage. Au Canada, cette information est stockée dans le Système mondial de gestion des cas (SMGC) à Citoyenneté et Immigration Canada (CIC). Il peut arriver à l'occasion — par exemple, en cas de changement de statut en matière d'immigration — qu'un deuxième dossier soit créé pour une personne. Le SMGC est programmé de façon à détecter ces « dossiers de client en double » pour s'assurer que les renseignements personnels périmés ou protégés ne sont pas communiqués aux autorités américaines.

À cinq reprises en 2014, lorsque les autorités américaines ont interrogé le système sur des clients qui avaient deux dossiers, le système a affiché les deux dossiers en raison d'un problème technique. Pour chaque personne touchée, l'un des dossiers mentionnait que le Canada avait refusé d'émettre un visa de séjour, tandis que l'autre indiquait que la personne avait le statut de résident permanent au Canada. Or, en vertu d'une entente conclue entre les deux pays, il est interdit de communiquer de l'information sur des citoyens ou des résidents permanents au Canada et aux États-Unis; le fait qu'un visa leur avait été refusé par le passé n'aurait donc pas dû être communiqué.

La première des cinq atteintes est survenue en avril 2014 — soit deux mois après que Citoyenneté et Immigration Canada avait modifié le SMGC pour corriger le problème en question —, mais elle n'a été constatée qu'en juillet, au cours d'une vérification manuelle qu'effectue CIC tous les trimestres aux fins de contrôle de la qualité.

À la suite des atteintes les plus récentes, Citoyenneté et Immigration Canada a appliqué une autre solution technique pour corriger le problème. Le ministère vérifie maintenant toutes les semaines les transactions avec les États-Unis. Si CIC avait instauré un calendrier de surveillance aussi rigoureux lorsqu'il a effectué la première correction, les atteintes survenues entre avril et juillet auraient pu être évitées. À l'issue de notre examen, nous avons recommandé au ministère de continuer à surveiller sur une base hebdomadaire les transactions avec les États-Unis pour s'assurer que le SMGC ne présente plus de problèmes techniques de cette nature. Nous lui avons aussi recommandé de prévoir, après tout

changement au système, une période de vérifications plus fréquentes afin de pouvoir corriger rapidement toute anomalie éventuelle.

CONSEIL NATIONAL DE RECHERCHES CANADA — INTRUSION DANS LE RÉSEAU

L'instauration de protocoles appropriés pour le traitement des renseignements personnels permet d'éviter l'erreur humaine, mais une atteinte majeure à la sécurité des données survenue au Conseil national de recherches du Canada (CNRC) fait ressortir l'importance de s'assurer que l'information n'est pas vulnérable aux points faibles de l'infrastructure de technologie de l'information (TI).

En juillet 2014, le CNRC a déclaré une intrusion dans son réseau informatique. En plus de mettre le réseau à l'arrêt pendant une longue période, il a informé le Commissariat que l'intrus avait peut-être pu consulter les renseignements personnels d'employés et de clients actuels et passés de l'organisme — soit environ 50 000 personnes en tout.

Au cours de notre examen, nous avons constaté que le CNRC avait déjà commencé à mettre en œuvre un plan d'action prévoyant notamment la reconstruction de son infrastructure de TI et le renforcement de la culture de sécurité au sein de l'organisme. Selon nous, le Commissariat n'avait aucune autre mesure à prendre à ce moment-là. Nous nous attendons à ce que le CNRC effectue les évaluations du risque d'atteinte à la sécurité qui s'imposent alors qu'il reconstruit son infrastructure et passe au nouveau système d'exploitation. Il devrait notamment prévoir une certification et une accréditation progressives de tous les systèmes et services et, au besoin, des évaluations des facteurs relatifs à la vie privée et des évaluations de la menace et du risque afin d'atténuer tous les risques d'atteinte à la vie privée décelés.

****

À mesure que l'activité numérique augmente et que les organismes publics continuent de trouver de nouvelles façons d'utiliser les renseignements personnels pour de nouvelles initiatives, il faut accorder une importance croissante à la sécurité de ces données.

Lorsqu'elles planifient de nouvelles initiatives, les institutions doivent être mises au courant des incidents antérieurs, comme ceux mentionnés dans le présent rapport, afin de mettre en œuvre des mesures proactives pour prévenir le plus possible les atteintes à la sécurité des données.

À cette fin, elles doivent non seulement protéger les données qu'elles recueillent, mais aussi gagner et maintenir la confiance des citoyens auxquelles elles fournissent leurs services.

Vérification : protection des renseignements personnels et dispositifs de stockage portables

POINTS SAILLANTS

L'utilisation des dispositifs de stockage portables (DSP) est très répandue au sein des institutions fédérales. Malgré les politiques, les processus et les contrôles entourant leur utilisation, il y a d'importantes possibilités d'améliorer la gestion et la protection de ces dispositifs. Ainsi, parmi les entités sélectionnées aux fins d'examen :

- environ 70 % n'avaient pas évalué en bonne et due forme les risques associés à l'utilisation de tous les types de DSP;
- plus de 90 % n'avaient pas fait l'inventaire et le suivi de l'ensemble de ces dispositifs tout au long de leur cycle de vie;
- plus de 85 % ne tenaient pas de registre confirmant que les données conservées sur les DSP excédentaires ou défectueux avaient été détruites de façon sécuritaire;
- environ 55 % n'avaient pas évalué les risques d'atteinte à la sécurité des renseignements personnels qui résultent de l'absence de contrôles visant à empêcher l'utilisation de DSP non autorisés.

Il existe un registre des téléphones intelligents actifs, mais l'identité des utilisateurs n'est généralement pas connue. De plus, des contrôles normalisés doivent encore être mis en place de façon uniforme.

Les entités fédérales qui autorisent l'utilisation des DSP sans avoir mis en place les contrôles appropriés s'exposent à plusieurs risques :

- perte de données confidentielles ou de renseignements personnels, ou accès non autorisé à cette information, ce qui porterait préjudice au gouvernement et aux citoyens;
- érosion de la confiance du public et risque élevé d'atteinte à la réputation;
- coûts considérables associés à la perte de données et aux efforts de récupération des données.

INTRODUCTION

Les DSP sont des accessoires électroniques servant au stockage des données numériques. En général, ils sont de petite taille et faciles à utiliser. Il peut s'agir, par exemple, d'ordinateurs portables, de tablettes électroniques, de téléphones intelligents, de disques durs externes, de clés USB et de disques optiques.

La capacité de stockage des DSP, de même que leur portabilité et leur facilité d'utilisation, en font des outils prisés et fort utiles. Dans bien des cas, il est rapide et facile d'y copier des données émanant des réseaux du gouvernement.

Les DSP présentent de nombreux avantages, mais ils posent aussi certains risques d'atteinte à la vie privée et à la sécurité. En raison de leur taille et de leur portabilité, ils peuvent facilement être perdus, égarés ou volés. L'utilisation de ces dispositifs peut accroître le risque de perte de données par une institution et, par le fait même, le risque d'accès non autorisé aux données. L'accès non autorisé aux données pourrait avoir de graves conséquences pour les personnes — pertes financières, atteinte à la réputation, atteinte à la sécurité personnelle, etc.

Lorsque l'information stockée sur un dispositif portable est sensible, les répercussions de la perte du dispositif peuvent être encore plus graves. Les risques d'atteinte à la vie privée découlant de la perte d'un dispositif de stockage portable au sein du gouvernement sont d'autant plus graves que les fonds de renseignements personnels de nature délicate du gouvernement sont très volumineux.

À la suite de nombreuses atteintes à la sécurité des données, notamment la perte, en 2012, d'un disque dur portable contenant des renseignements personnels concernant des bénéficiaires de prêts d'études, le Commissariat a annoncé son intention de vérifier les pratiques de gestion des DSP dans l'ensemble du gouvernement.

OBJECTIF DE LA VÉRIFICATION

La vérification visait à déterminer si les entités fédérales avaient mis en place des contrôles adéquats pour protéger les renseignements personnels stockés sur les DSP.

Afin d'éviter la perte ou le vol des données stockées sur les DSP, les entités fédérales utilisant ces dispositifs devraient avoir mis en place des mesures appropriées pour protéger les renseignements personnels. Selon nous, ces entités devraient être dotées d'un système de gouvernance à l'appui de la gestion et de l'utilisation des DSP. Elles devraient également avoir établi des processus administratifs pour faire l'inventaire et le suivi des DSP tout au long de leur cycle de vie. Plus important encore, elles devraient avoir mis en place des contrôles, entre autres des mesures de sécurité physiques et technologiques, pour assurer la

protection contre tout accès non autorisé aux données sensibles.

En mai 2014, soit six mois après le début de notre vérification, le Secrétariat du Conseil du Trésor du Canada a publié un *Avis de mise en œuvre de la Politique sur la technologie de l'information*[4] sur l'utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada. L'avis donne aux institutions des instructions sur la gestion des DSP, y compris la mise en place de contrôles physiques et de contrôles de sécurité. De nombreuses autres dispositions que renferme l'avis reflètent les attentes énoncées pour les besoins de la vérification et confirment l'importance de protéger les DSP et l'information qui y est conservée.

SÉLECTION DES ENTITÉS VÉRIFIÉES

Au début de notre vérification, nous avons effectué un sondage auprès de 49 entités fédérales. Les participants, sélectionnés en raison du type de renseignements personnels qu'ils détiennent, devaient répondre à une série de questions concernant leur utilisation des DSP. Les questions portaient sur trois secteurs précis : les contrôles physiques, les contrôles de sécurité ainsi que la gestion de la protection de la vie privée et la responsabilisation.

À la lumière des réponses obtenues, nous avons retenu 16 entités aux fins d'examen. Plusieurs facteurs ont été pris en compte à cet égard, y compris l'ampleur du déploiement des DSP au sein de l'institution, le volume de renseignements personnels détenus et leur sensibilité, l'existence — ou l'absence — de contrôles visant à protéger les renseignements personnels stockés sur les DSP et l'utilisation de DSP personnels à des fins professionnelles.

Services partagés Canada (SPC) a été ajouté aux 16 entités retenues du fait que ce ministère est chargé de la gestion des centres de données (p. ex, les serveurs réseau) et des services de télécommunications (p. ex., la distribution des téléphones intelligents) au nom de 43 institutions fédérales. L'examen a porté principalement sur le rôle de SPC à cet égard.

OBSERVATIONS

Les résultats de la vérification sont présentés ci-après. Soulignons toutefois que certaines observations ne visent pas toutes les entités. Pour obtenir plus de détails, les lecteurs peuvent consulter les rapports d'examen sommaire de la vérification, qui sont affichés sur le site Web du Commissariat. Toutes les entités ont accepté les recommandations issues de la vérification et convenu d'y donner suite.

4 https://www.tbs-sct.gc.ca/it-ti/itpin-ampti/2014-01-fra.asp.

La plupart des entités n'avaient établi aucun processus administratif pour faire l'inventaire et le suivi de chacun des types de dispositifs de stockage portables tout au long de leur cycle de vie.

Toutes les entités enregistrent les ordinateurs portables et les tablettes électroniques qu'elles fournissent et en font le suivi. En revanche, pour ce qui est de la gestion des dispositifs de stockage USB — disques durs portables et clés USB — ainsi que des CD et des DVD, les processus administratifs étaient dans une large mesure inexistants ou au début de leur mise en œuvre. Par conséquent, on connaît peu l'ampleur de l'utilisation de ces dispositifs.

En l'absence de processus administratif officiel pour faire le suivi de tous les DSP, il a été impossible de déterminer l'ampleur du déploiement des dispositifs appartenant au gouvernement ainsi que les fins visées. Il est également difficile de confirmer si les dispositifs sont restitués à la fin de leur cycle de vie (notamment lorsque des employés quittent une organisation). La plupart des entités ont mis en place des procédures pour la destruction sécuritaire des données stockées sur les DSP défectueux, restitués ou excédentaires. Toutefois, faute de mécanisme de suivi officiel, on n'a aucune garantie que tous les DSP sont nettoyés et qu'ils ne contiennent plus de données de l'institution ni de renseignements personnels avant leur élimination.

Les institutions fédérales ont l'obligation de protéger les renseignements personnels qui leur sont confiés. Elles doivent donc savoir où sont conservés les renseignements, si bien que l'enregistrement et le suivi des DSP sont essentiels à cette fin. En l'absence de ce type de mécanisme, les institutions ne sont pas en mesure de déterminer quels dispositifs sont utilisés, par qui et à quelles fins, ce qui restreint par le fait même la capacité à atténuer le plus possible le risque de perte de données.

D'après nos observations préliminaires sur les risques associés à la perte de données ou à l'accès non autorisé à des renseignements personnels, le fait qu'il n'existe aucune liste faisant état de tous les types de DSP constitue un risque potentiel d'atteinte à la vie privée des Canadiens.

La plupart des entités avaient adopté un cadre pour l'élimination sécuritaire des dispositifs de stockage portables à l'appui de leur gestion, mais on constate des lacunes à cet égard.

Une méthode d'élimination sécuritaire garantit que l'information ne pourra pas être récupérée ou reconstituée. Dans le cas des DSP, il faut nettoyer le dispositif au moyen d'un mécanisme de nettoyage sécurisé (certifié) ou le détruire physiquement.

La plupart des entités s'étaient dotées de processus officiels pour éliminer les DSP excédentaires ou défectueux. Plusieurs d'entre elles avaient adopté une approche centralisée selon

laquelle les dispositifs non nettoyés provenant de divers sites devaient être acheminés à un endroit central aux fins d'élimination. Cette façon de procéder présente un risque d'accès aux données en cas de perte ou de vol des dispositifs en transit. À l'exception d'une entité qui avait adopté un processus d'élimination centralisé, ce risque n'a pas été évalué.

Rien n'indique que les entités éliminent les DSP de façon non sécuritaire, mais la quasi-totalité d'entre elles n'ont pas comme pratique courante de conserver des preuves documentaires pour confirmer la destruction de toutes les données stockées sur les dispositifs excédentaires ou défectueux. Ces éléments probants permettent à une organisation de montrer qu'elle a exercé la diligence voulue pour s'assurer que les renseignements personnels sont éliminés de manière sécuritaire.

De nombreuses entités n'avaient pas évalué les risques d'atteinte à la vie privée associés à certains types de dispositifs de stockage portables.

Afin de se doter d'une structure de gouvernance efficace pour la gestion des DSP, il est essentiel d'évaluer pleinement le risque associé à leur utilisation. On doit notamment déterminer si le risque d'atteinte à la vie privée et à la sécurité en découlant est proportionné aux avantages connexes. Ce type d'analyse appuie la décision de déployer des DSP et les conditions de leur déploiement ainsi que la mise en place des contrôles de sécurité appropriés pour protéger les renseignements personnels. L'analyse pourrait également avoir une incidence sur l'élaboration de processus de gestion de l'inventaire des DSP ainsi que de programmes de formation et de sensibilisation des employés.

À quelques exceptions près, les entités avaient mené à bien des analyses du risque associé à l'utilisation des ordinateurs portables, des tablettes électroniques et des dispositifs de stockage USB. Toutefois, la majorité d'entre elles n'avaient pas analysé le risque d'atteinte à la sécurité des renseignements personnels qui découle de l'absence de contrôles techniques portant sur le branchement de dispositifs de stockage USB non autorisés et l'utilisation de CD et de DVD pour stocker des données. Dans certains cas, l'analyse du risque avait fait abstraction de la capacité de télécharger des applications non autorisées sur les dispositifs et de les utiliser.

De nombreuses entités n'avaient pas mis en place de contrôles adéquats pour se protéger contre tout accès non autorisé aux données sensibles conservées sur des dispositifs de stockage USB.

Les mesures de sécurité physiques et logicielles assurent la protection et la confidentialité des renseignements personnels conservés sur les DSP. Les ordinateurs portables et les tablettes électroniques sont généralement dotés de fonctions de cryptage, de paramètres robustes pour les mots de passe ainsi que de contrôles

visant à empêcher l'installation d'applications non autorisées. En revanche, les autres DSP présentent des lacunes au chapitre des mesures de sécurité et des contrôles visant à protéger les données qui y sont conservées. Malgré la gamme de solutions de cryptage offertes pour les logiciels et le matériel, le quart des entités n'exigeaient pas l'utilisation de dispositifs de stockage USB cryptés. En outre, les deux tiers n'avaient pas mis en place de contrôles technologiques empêchant le branchement de DSP non autorisés (p. ex., des dispositifs personnels) à leurs réseaux.

La mise en place de contrôles logiciels adéquats est essentielle pour protéger les données stockées sur les DSP. En l'absence de ce type de contrôles, le risque d'accès non autorisé aux renseignements personnels se trouve accru, ce qui pourrait porter préjudice aux parties touchées et miner la confiance du public dans la capacité d'une institution à protéger les renseignements personnels.

Les entités s'étaient dotées d'un cadre stratégique pour appuyer la gestion des dispositifs de stockage portables.

Des politiques robustes sont essentielles à la protection des biens organisationnels, y compris les renseignements personnels. Elles établissent une reddition de compte et les responsabilités connexes, et procurent le mécanisme qui intègre la sécurité et la protection des renseignements personnels aux activités courantes. L'absence de politiques bien définies peut conduire à des pratiques de traitement de l'information non uniformes et inadéquates, susceptibles de porter atteinte à la vie privée.

Les entités vérifiées avaient mis en place une politique — ou une série de politiques — régissant la gestion et l'utilisation des DSP. Ces outils de gouvernance imposent les critères d'utilisation et de protection adéquates des DSP. En règle générale, les rôles et les responsabilités en matière de gestion des DSP étaient bien définis et la responsabilité relative à leur utilisation était clairement établie.

Toutefois, certaines lacunes ont été cernées. Nous nous attendions à ce que les politiques abordent à tout le moins l'utilisation de tous les types de DSP, l'obligation de protéger ces dispositifs et l'information qui y est conservée, l'obligation de signaler la perte ou le vol d'un dispositif, ainsi que l'utilisation de dispositifs personnels à des fins professionnelles. Les politiques mises en place par le quart des entités faisaient abstraction d'un ou de plusieurs de ces aspects.

L'efficacité d'une politique — ou d'une série de politiques — peut être évaluée en partie selon la mesure dans laquelle les employés en connaissent la teneur. Toutes les entités, sauf une, avaient mis en œuvre des programmes de formation qui comportaient des modules portant sur l'utilisation des DSP. Il y a toutefois matière à amélioration à ce chapitre. Plus précisément, dans environ le quart des entités,

la participation des employés aux programmes de formation offerts n'était pas obligatoire. Parmi les autres lacunes dignes de mention, signalons le matériel de formation qui ne couvrait pas tous les types de DSP, la perte ou le vol de dispositifs et la politique régissant l'utilisation de dispositifs personnels ou l'interdiction de leur utilisation.

Les employés doivent bien connaître les politiques et les procédures complémentaires de l'organisation portant sur l'utilisation des DSP, sans quoi il existe un risque qu'ils n'exercent pas la diligence voulue dans la gestion des renseignements personnels stockés sur des DSP. Cela pourrait mener à une atteinte à la vie privée.

Le registre central des utilisateurs de téléphones intelligents du gouvernement est incomplet.

Services partagés Canada (SPC) assure la gestion des téléphones intelligents pour 43 institutions fédérales (appelées « organisations partenaires »). Sur ce nombre, 10 ont été sélectionnées aux fins de notre vérification.

En vertu de son mandat, SPC a élaboré un registre pour suivre la remise de tous les nouveaux dispositifs. Ce mécanisme vise à consigner intégralement tous les téléphones intelligents actifs au sein des organisations partenaires. À l'heure actuelle, les dispositifs actifs ne figurent pas tous dans le registre.

D'après SPC, au moment de la transition (c'est-à-dire du transfert de la responsabilité de la gestion des téléphones cellulaires des organisations partenaires), on ne lui a pas fourni de listes exhaustives des utilisateurs de téléphones intelligents des organisations partenaires. Le ministère a lancé de nombreuses initiatives pour mettre à jour le registre. Toutefois, selon toute vraisemblance, la liste des utilisateurs de téléphones intelligents ne sera pas complète avant septembre 2016 malgré les efforts déployés par SPC.

Les organisations sont tenues de protéger les renseignements personnels tout au long de leur cycle de vie, peu importe le mode de stockage. L'absence d'un mécanisme permettant d'enregistrer les utilisateurs de téléphones intelligents réduit la capacité d'une institution à s'assurer que les dispositifs sont gérés conformément à la politique établie — y compris la remise des dispositifs qui ne servent plus. Sans cette assurance, il y a un risque que les dispositifs ne soient pas nettoyés de façon sécuritaire, ce qui pourrait entraîner des accès non autorisés aux renseignements personnels.

Aucun contrôle de sécurité uniforme n'avait encore été mis en place pour la gestion des téléphones intelligents enregistrés.

Avant la création de SPC, la gestion des stocks de téléphones intelligents relevait des organisations partenaires, qui devaient notamment établir et mettre en œuvre des paramètres de sécurité pour protéger les données stockées sur les appareils. Les

paramètres établis par les 10 organisations partenaires sélectionnées ont été examinés dans le cadre de la vérification. Trois des entités avaient mis en place des contrôles rigoureux, mais nous avons constaté des points faibles dans les paramètres de sécurité des sept autres. Ces points faibles existaient déjà lorsque SPC a pris en charge la gestion des téléphones intelligents.

Services partagés Canada a adopté une approche en plusieurs étapes dans le cadre du transfert de la responsabilité de la gestion des téléphones intelligents, y compris les paramètres de sécurité. Il a établi de nombreux profils de configuration à cet égard; tous les profils prévoient des contrôles de base (p. ex., cryptage et paramètres robustes pour les mots de passe).

À la fin de notre vérification, les paramètres de base n'avaient pas été installés sur tous les appareils. D'ailleurs, ils pourraient ne pas être mis en œuvre avant septembre 2016 dans certains cas. Entre-temps, on ne remédie pas aux lacunes et aux points faibles connus sur le plan de la sécurité, ce qui entraîne un risque d'accès aux données stockées sur les appareils visés.

Les risques découlant du branchement de dispositifs de stockage USB non autorisés aux serveurs réseau n'ont pas été évalués.

Services partagés Canada gère les serveurs réseau au nom des organisations partenaires. Ces serveurs peuvent contenir une quantité considérable de renseignements personnels. Aucun contrôle technologique n'a été mis en place pour prévenir le transfert de cette information sur des dispositifs de stockage USB non autorisés (p. ex., des dispositifs non dotés des fonctions de sécurité imposées par l'organisation). Compte tenu du volume de données stockées sur bon nombre de ces serveurs et de leur degré de sensibilité, l'accès non autorisé aux données découlant de l'utilisation de ces dispositifs pourrait avoir des répercussions négatives pour des milliers de personnes et pour le gouvernement.

CONCLUSION

Les atteintes à la vie privée rapportées dans les médias ont sensibilisé les gens et les organisations aux risques d'atteinte à la protection des données associés à l'utilisation des DSP, mais le risque de perte ou de communication involontaire de renseignements personnels demeure une réelle possibilité. La solution ne consiste pas ici à empêcher ou à interdire l'utilisation de ces dispositifs au sein de l'administration publique. Bien au contraire. À une époque où les employés sont de plus en plus mobiles, les DSP s'avèrent des outils importants et fort utiles.

Nous avons entrepris une vérification horizontale pour évaluer les pratiques actuelles entourant l'utilisation des DSP au sein de certaines organisations fédérales.

Les entités avaient mis en place des cadres de gestion des DSP, mais il faut encore améliorer les contrôles — y compris les politiques, les procédures et les processus — pour protéger la vie privée. L'ampleur des améliorations qui s'imposent varie d'une entité à l'autre. De nombreuses observations s'appliquent toutefois à la plupart d'entre elles, notamment l'absence d'analyse des risques et de mécanisme de suivi des stocks de tous les types de dispositifs ainsi que la tenue de registres confirmant que les données stockées sur les dispositifs excédentaires ou défectueux ont été détruites de façon sécuritaire. Ces lacunes, ainsi que les autres lacunes et points faibles mentionnés, pourraient avoir des répercussions sur la protection de la vie privée. En y remédiant, les entités pourraient atténuer les risques d'atteinte à la sécurité des renseignements personnels transférés ou conservés sur les DSP.

SUIVI

Notre méthode de vérification prévoit un suivi dans deux ans auprès des 17 entités retenues aux fins d'examen. Nous évaluerons alors les progrès réalisés dans la mise en œuvre des recommandations issues de la vérification.

Comme nous l'avons mentionné, le Secrétariat du Conseil du Trésor a publié en mai 2014 un *Avis de mise en œuvre de la Politique sur la technologie de l'information* sur l'utilisation sécurisée des supports de stockage de données portatifs dans l'ensemble de l'administration fédérale. Au sein des institutions auxquelles il s'adresse, cet avis devrait constituer une référence en matière de protection de la vie privée et de gestion des DSP. Nous encourageons les institutions à donner suite à l'avis et à assurer la conformité à la politique.

AU SUJET DE LA VÉRIFICATION

Autorisation législative

L'article 37 de la *Loi sur la protection des renseignements personnels* confère au commissaire à la protection de la vie privée du Canada le pouvoir d'examiner les pratiques des institutions fédérales en matière de traitement des renseignements personnels.

Objectif

L'objectif de la vérification était de déterminer si les entités sélectionnées avaient mis en place des contrôles adéquats – y compris des politiques, des procédures et des processus – pour protéger les renseignements personnels transférés ou conservés sur des DSP.

Critères

Les critères de vérification ont été définis à partir de la *Loi sur la protection des renseignements personnels* et des politiques, directives et normes du Secrétariat du Conseil du Trésor du Canada sur la gestion des renseignements personnels.

Nous nous attendions à ce que les entités aient :

- fait l'évaluation des risques d'atteinte à la vie privée et à la sécurité découlant de l'utilisation des DSP;
- mis en place de contrôles physiques et logiciels adéquats pour protéger les renseignements personnels transférés ou stockés sur ces dispositifs;
- établi des politiques et de procédures — régissant l'utilisation des DSP — conformes aux exigences et aux pratiques exemplaires du gouvernement du Canada en matière de sécurité;
- mis en place des procédures officielles pour éliminer de façon sécuritaire les DSP excédentaires ou défectueux;
- pris des mesures pour faire connaître aux employés les utilisations acceptables des DSP et les risques associés à ces dispositifs;
- mis en œuvre des procédures d'intervention en cas d'atteinte à la sécurité des données (communication inappropriée de renseignements personnels) découlant de la perte ou du vol de DSP.

Portée et approche

Dans le cadre de la planification de la vérification, nous avons évalué la nature, l'ampleur et la sensibilité des renseignements personnels détenus par des institutions fédérales en utilisant à cette fin la description de leurs fonds de renseignements personnels respectifs. Par suite de cette analyse, nous avons demandé à 49 institutions de participer à un sondage.

Le sondage avait pour but d'aider à sélectionner les organisations qui feraient l'objet de la vérification. Nous avons conçu à cette fin un outil d'évaluation du risque. Après avoir attribué une pondération à chaque question en fonction de son importance relative, nous avons évalué les réponses des participants selon une échelle de notation, puis additionné les résultats de chaque institution pour obtenir son score total. Les institutions ont ensuite été classées dans l'une des cinq catégories établies.

Le cas échéant, nous avons utilisé les critères de sélection suivants pour les institutions d'une même catégorie :

- le volume de renseignements personnels détenus par l'organisation et leur sensibilité — et, par le fait même, les répercussions éventuelles d'une atteinte à la sécurité des données ou d'un accès non autorisé aux données;
- le nombre et le type de DSP distribués par l'organisation;
- les cadres de contrôle en place pour protéger les renseignements personnels conservés sur les DSP.

Pour les besoins de la vérification, nous avons utilisé divers moyens afin d'obtenir les éléments probants, entre autres des observations sur place, des entretiens et des renseignements obtenus par correspondance. Nous avons aussi examiné les politiques et les procédures, les évaluations de la menace et du risque ainsi que le matériel de formation.

La vérification s'est déroulée principalement à l'administration centrale des entités. Des activités d'examen ont également eu lieu à certains endroits dans les régions, dans les cas où la responsabilité de la gestion des DSP était décentralisée. Les travaux d'examen étaient pour l'essentiel terminés le 28 novembre 2014.

Normes

La vérification a été effectuée conformément au mandat législatif, aux politiques et aux pratiques du Commissariat à la protection de la vie privée du Canada et à l'esprit des normes de vérification recommandées par l'Institut Canadien des Comptables Agréés.

Équipe de vérification

Steven Morgan – directeur général
Dan Bourgeault
Garth Cookshaw
Sylvie Gallo Daccash
Michael Fagan
Gaétan Létourneau
Anne Overton
Kyle Sprysa
Bill Wilson

LISTE DES PARTICIPANTS AU SONDAGE

	Nom de l'institution
1	Administration canadienne de la sûreté du transport aérien
2	Affaires autochtones et Développement du Nord Canada
3	Affaires étrangères, Commerce et Développement Canada
4	Agence canadienne d'inspection des aliments
5	Agence de la santé publique du Canada
6	Agence de promotion économique du Canada atlantique
7	Agence des services frontaliers du Canada
8	Agence du revenu du Canada
9	Agriculture et Agroalimentaire Canada
10	Anciens Combattants Canada
11	Banque de développement du Canada
12	Banque du Canada
13	Bibliothèque et Archives Canada
14	Bureau de l'enquêteur correctionnel
15	Bureau de l'ombudsman des contribuables
16	Bureau de l'Ombudsman du ministère de la Défense nationale et des Forces canadiennes
17	Bureau de la sécurité des transports du Canada
18	Citoyenneté et Immigration Canada
19	Comité de surveillance des activités de renseignement de sécurité
20	Comité externe d'examen des griefs militaires
21	Commissariat à l'intégrité du secteur public du Canada
22	Commissariat au lobbying du Canada
23	Commission canadienne des droits de la personne
24	Commission d'examen des plaintes concernant la police militaire
25	Commission de l'immigration et du statut de réfugié du Canada
26	Commission de la capitale nationale
27	Commission des libérations conditionnelles du Canada
28	Commission des plaintes du public contre la GRC
29	Diversification de l'économie de l'Ouest Canada
30	Élections Canada
31	Emploi et Développement social Canada
32	Financement agricole Canada
33	Gendarmerie royale du Canada
34	Justice Canada
35	Office des transports du Canada
36	Pêches et Océans Canada
37	Santé Canada

38	Service canadien du renseignement de sécurité
39	Service correctionnel Canada
40	Services partagés Canada
41	Société canadienne d'hypothèques et de logement
42	Société canadienne des postes
43	Société d'assurance-dépôts du Canada
44	Statistique Canada
45	Transports Canada
46	Travaux publics et Services gouvernementaux Canada
47	Tribunal de la sécurité sociale du Canada
48	Tribunal des anciens combattants (révision et appel)
49	VIA Rail Canada

Pour lire les rapports préparés por chacune des entités véfifiée, allez à :
https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_f.asp

LISTE DES ENTITÉS SÉLECTIONNÉES AUX FINS DE L'EXAMEN

	Nom de l'institution
1	Affaires autochtones et Développement du Nord Canada (AADNC)
2	Agence de la santé publique du Canada (ASPC)
3	Agence des services frontaliers du Canada (ASFC)
4	Agence du revenu du Canada (ARC)
5	Agriculture et Agroalimentaire Canada (AAC)
6	Banque de développement du Canada (BDC)
7	Banque du Canada (BdC)
8	Citoyenneté et Immigration Canada (CIC)
9	Commission canadienne des droits de la personne (CCDP)
10	Commission de l'immigration et du statut de réfugié du Canada (CISRC)
11	Commission des libérations conditionnelles du Canada (CLCC)
12	Financement agricole Canada (FAC)
13	Pêches et Océans Canada (MPO)
14	Services partagés Canada (SPC)
15	Société canadienne d'hypothèques et de logement (SCHL)
16	Société d'assurance-dépôts du Canada (SADC)
17	Statistique Canada (StatCan)

TABLEAU SOMMAIRE DES RECOMMANDATIONS COMMUNES

Recommandations	AAC	AADNC	ARC	ASFC	ASPC	BDC	BdC	CCDP	CIC	CISRC	CLCC	FAC	MPO	SADC	SCHL	StatCan
Veiller à ce que la remise de tous les dispositifs de stockage portables — qui peuvent servir à conserver des renseignements personnels — soit consignée à des fins d'identification et de suivi.	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●
Conserver des preuves documentaires — soit le rapport de confirmation généré par le mécanisme de nettoyage certifié, soit la confirmation de destruction du matériel — en tant que vérification visant à assurer que toutes les données sur les dispositifs de stockage portables excédentaires ou défectueux ont été éliminées de manière sécuritaire.	●	●			●	●	●	●	●	●	●	●	●	●	●	●
Évaluer le processus d'élimination actuel — pour ce qui est de l'expédition des dispositifs de stockage portables excédentaires ou défectueux vers un site central (p. ex., le siège social) — pour garantir que des mesures de contrôle adéquates sont en place pour atténuer le risque d'accès aux données.				●		●	●	●	●	●	●	●		●	●	●

Recommandations	AAC	AADNC	ARC	ASFC	ASPC	BDC	BdC	CCDP	CIC	CISRC	CLCC	FAC	MPO	SADC	SCHL	StatCan
Évaluer le risque d'atteinte à la protection de renseignements personnels résultant de l'absence de contrôles concernant le branchement de dispositifs de stockage USB non autorisés, et mettre en place les mesures nécessaires pour corriger les lacunes et les faiblesses cernées.	●	●		●		●		●			●		●	●	●	
Évaluer le risque d'atteinte à la protection de renseignements personnels résultant de l'utilisation de CD/DVD pour stocker des données et mettre en place les mesures nécessaires pour corriger les lacunes et les faiblesses cernées.	●	●		●	●	●		●		●	●	●	●	●		
Veiller à ce que tous les dispositifs de stockage portables susceptibles d'être utilisés pour stocker des renseignements personnels soient dotés d'une fonction de cryptage.	●	●				●		●	●		●			●		

Recommandations	AAC	AADNC	ARC	ASFC	ASPC	BDC	BdC	CCDP	CIC	CISRC	CLCC	FAC	MPO	SADC	SCHL	StatCan
S'assurer que tous les employés, y compris le personnel contractuel, connaissent les politiques qui régissent l'utilisation des dispositifs de stockage portables, et fournir des conseils pour atténuer les risques pour la vie privée inhérents à l'utilisation de ces dispositifs.						●		●	●		●	●	●	●	●	●

Recommandations visant expressément Services partagés Canada	
En collaboration avec les organisations partenaires, faire en sorte que tous les téléphones intelligents actifs soient enregistrés, soit par nom d'utilisateur ou par nom de personne-ressource, d'ici janvier 2016.	●
Veiller à ce que des contrôles de sécurité de base soient mis en œuvre sur tous les téléphones intelligents utilisés par les organisations partenaires d'ici janvier 2016.	●
Évaluer les risques pour les renseignements personnels qui découlent d'une absence de contrôles pour empêcher le branchement de dispositifs USB non autorisés sur les serveurs et mettre en place des contrôles appropriés pour corriger les vulnérabilités et les faiblesses relevées.	●

Bilan de l'exercice

Évaluations des facteurs relatifs à la vie privée

Les évaluations des facteurs relatifs à la vie privée (EFVP) servent à déceler les risques d'atteinte à la vie privée qui pourraient être associés aux programmes ou aux services fédéraux nouveaux ou remaniés. Selon la *Directive sur l'évaluation des facteurs relatifs à la vie privée* publiée par le Secrétariat du Conseil du Trésor du Canada (SCT), les institutions fédérales doivent effectuer une EFVP à l'égard des activités ou des programmes nouveaux ou ayant subi des modifications importantes, lorsque ceux-ci font appel à des renseignements personnels dans le cadre d'un processus décisionnel touchant des individus. Elles doivent faire la preuve que les risques d'atteinte à la vie privée ont été cernés et atténués de façon efficace.

Les institutions remettent au SCT et au Commissariat une copie de leurs EFVP. Le Commissariat examine ces évaluations et, s'il y a lieu, donne aux institutions des conseils sur les mesures à prendre pour améliorer leurs pratiques de traitement des renseignements personnels. Les recommandations du Commissariat ne sont pas contraignantes mais, dans la plupart des cas, les institutions acceptent et mettent en œuvre ses conseils.

En 2014-2015, le Commissariat a reçu 70 nouvelles EFVP et terminé l'examen de 73 dossiers. Il a transmis des recommandations détaillées pour 51 EFVP portant sur des initiatives susceptibles de présenter un risque élevé d'atteinte à la vie privée et pour 22 activités considérées comme étant à risque faible.

Le Commissariat a aussi ouvert 19 nouveaux dossiers de consultations et donné des conseils à plusieurs institutions fédérales sur les risques d'atteinte à la vie privée associés à de nombreuses initiatives encore aux premiers stades de leur développement. Mentionnons notamment les projets visant à tester l'utilisation de la technologie de reconnaissance faciale à la frontière canadienne, ceux visant à rendre obligatoire la déclaration du numéro d'assurance sociale dans le cadre du recensement, ainsi que les initiatives destinées à accroître l'utilisation, par le gouvernement, d'information provenant de sources accessibles au public, y compris les fils d'actualité publics dans les médias sociaux.

Les résumés ci-après donnent un aperçu de certaines EFVP prioritaires que le Commissariat a examinées en 2014-2015.

Agence des services frontaliers du Canada — Initiative sur les entrées et les sorties

Comme nous le faisons depuis plusieurs années, nous avons examiné les EFVP associées à de nombreux programmes et activités se rapportant à l'initiative canado-américaine Par-delà la frontière et mené des consultations à ce sujet, y compris des consultations auprès de Sécurité publique Canada et de l'Agence des services frontaliers du Canada (ASFC) sur la mise en œuvre des prochaines phases de l'Initiative sur les entrées et les sorties.

Dans le cadre des phases I et II de cette initiative, l'ASFC et le département de la Sécurité intérieure des États-Unis ont commencé à recueillir respectivement l'information sur l'entrée de ressortissants de pays tiers et de résidents permanents qui franchissent la frontière par voie terrestre. La phase III (qui n'est pas encore mise en œuvre) étendrait la surveillance aux citoyens canadiens et américains franchissant la frontière par voie terrestre.

Au cours de la phase IV, l'ASFC prévoit d'élargir le champ d'application du programme pour recueillir de l'information sur les personnes, y compris les citoyens canadiens, qui quittent le Canada par voie aérienne. Le gouvernement du Canada utilisera ces données à différentes fins au pays, notamment pour faire appliquer la loi et déterminer le traitement fiscal et l'admissibilité à des prestations sociales qui sont fondés sur des critères de résidence. L'information sur les sorties pourra aussi être communiquée aux États-Unis et à d'autres pays au cas par cas.

Au moins cinq institutions fédérales prévoient des initiatives qui feraient appel à cette information — l'Agence des services frontaliers du Canada, l'Agence du revenu du Canada, le Service canadien du renseignement de sécurité, Citoyenneté et Immigration Canada, Emploi et Développement social Canada et la Gendarmerie royale du Canada. Nous attendons de recevoir les EFVP de ces institutions pour chacune des nouvelles utilisations qu'elles proposent.

Agence des services frontaliers du Canada — Utilisation accrue de la technologie de reconnaissance faciale

L'ASFC a consulté le Commissariat en 2014-2015 concernant son intention d'utiliser la technologie de reconnaissance faciale à tous les points d'entrée au pays. Le système compare les caractéristiques faciales des voyageurs entrants avec les photos d'individus inadmissibles au Canada

qui figurent sur les listes de surveillance de l'ASFC. L'Agence mène aussi des projets pour évaluer l'efficacité de la technologie dans des situations réelles à la frontière ainsi que dans diverses conditions d'éclairage et de mouvement de foule.

Nous avons donné des avis de haut niveau sur les risques d'atteinte à la vie privée, notamment celui de « faux positifs », qui pourraient entraîner une vérification secondaire et un examen minutieux injustifiés pour certaines personnes. Nous avons également souligné que l'ASFC devait entreprendre une évaluation de la menace et du risque (EMR) afin d'examiner les risques techniques ainsi que les risques d'atteinte à la vie privée et les répercussions connexes qu'il faudra prendre en compte au cours de l'évaluation de la nécessité et de l'efficacité de la technologie. Le Commissariat continuera de consulter l'ASFC dans ce dossier à mesure que les essais de validation de principe et les analyses subséquentes permettront d'en apprendre davantage.

Agence des services frontaliers du Canada — Ciblage fondé sur des scénarios

En 2014-2015, nous avons examiné une EFVP menée par l'ASFC portant sur l'adoption du ciblage fondé sur des scénarios, nouvelle méthode d'évaluation du niveau de risque des voyageurs entrant au Canada par voie aérienne.

En vertu de la loi canadienne, tous les transporteurs aériens commerciaux sont tenus de fournir à l'Agence une série de renseignements sur chaque personne qui entre au Canada, entre autres son nom, sa date de naissance, sa citoyenneté, un numéro de téléphone où la joindre, son numéro de siège et l'information sur le paiement. L'ASFC entre alors dans le Système d'information sur les voyageurs (SIPAX) les données recueillies et s'en sert pour identifier les individus qui sont ou pourraient être impliqués dans le terrorisme ou des activités criminelles liées au terrorisme ou encore dans d'autres infractions graves de nature transnationale.

Par le passé, l'Agence utilisait une méthode d'évaluation du risque individuelle reposant sur l'analyse de voyageurs particuliers, auxquels elle attribuait un niveau de risque en fonction des éléments d'information qui leur étaient propres. Les voyageurs présentant un niveau de risque élevé étaient détectés et faisaient l'objet d'un examen approfondi.

La nouvelle méthode reposant sur des scénarios a recours à l'analyse des mégadonnées pour évaluer tous les renseignements recueillis auprès des transporteurs aériens en fonction d'une série de conditions ou de scénarios. Ce système,

conçu de manière à assurer l'harmonisation avec celui utilisé aux États-Unis, pourrait permettre à l'exploitant, par exemple, de rechercher tous les ressortissants égyptiens de sexe masculin âgés de 18 à 20 ans qui se sont rendus à la fois à Paris et à New York. Cette nouvelle méthode inquiète le Commissariat du fait que l'on peut désormais cibler les voyageurs pour les soumettre à un examen approfondi s'ils correspondent aux caractéristiques générales d'un groupe — et que des personnes peuvent faire l'objet d'une attention récurrente et non nécessaire à la frontière en raison de caractéristiques qu'il leur est impossible de modifier, par exemple, l'âge, le sexe, la nationalité, le lieu de naissance et l'origine raciale ou ethnique.

À l'issue de l'examen de l'EFVP, nous avons formulé de nombreuses recommandations, entre autres :

- faire la preuve de la nécessité du ciblage fondé sur des scénarios, au-delà de l'objectif général d'harmonisation du système canadien avec celui des États-Unis;
- dans un souci de transparence, ajouter à l'EFVP une description générale des types de scénarios qui pourraient être utilisés pour identifier des voyageurs susceptibles de présenter un risque élevé;
- examiner régulièrement l'efficacité et la proportionnalité des scénarios, notamment les répercussions sur les libertés civiles et les droits de la personne;
- préparer une EFVP pour tout le Programme d'information préalable sur les voyageurs et du dossier passager, utilisé pour recueillir de l'information sur les voyageurs auprès des transporteurs aériens.

Nous avons constaté avec plaisir que l'ASFC avait donné suite à toutes nos recommandations. Elle devrait d'ailleurs nous présenter une EFVP plus détaillée sur l'ensemble des activités de collecte, d'analyse, d'utilisation et de communication d'information sur les voyageurs en 2015-2016.

Statistique Canada — Tests pour le Recensement de 2016

Statistique Canada (StatCan) fait le recensement de la population canadienne tous les quatre ans. Pour le recensement prévu en mai 2016, le ministère a envisagé de rendre obligatoire la déclaration du numéro d'assurance sociale (NAS). On établirait un lien entre ce numéro et les bases de données de l'Agence du revenu du Canada pour vérifier le niveau de revenu déclaré sur le questionnaire de recensement.

Nous avons recommandé à StatCan de déterminer s'il est nécessaire d'imposer la collecte du NAS à cette fin. Dans le recensement de 2011, le ministère demandait aux répondants l'autorisation de relier les données du recensement avec l'information sur le revenu en utilisant leurs données biographiques. D'après StatCan, 89 % des répondants ont donné leur consentement. Étant donné ce taux de réussite, nous avons exprimé des doutes sur la nécessité de remplacer cette méthode par la collecte obligatoire du NAS.

Depuis, StatCan nous a fait savoir que la déclaration obligatoire du NAS dans son Test du Programme du Recensement de 2014 a montré des gains négligeables au chapitre de l'efficacité et de la qualité des liens établis, ce qui ne justifierait pas la collecte obligatoire de ce numéro sur le questionnaire de recensement de 2016. Le ministère nous a donc informés qu'il n'imposerait pas cette exigence.

Gendarmerie royale du Canada — Banque nationale de données génétiques

La Banque nationale de données génétiques a été créée en 2000 pour établir et stocker le profil génétique des personnes reconnues coupables de certains crimes graves. Les modifications apportées en décembre 2014 à la *Loi sur l'identification par les empreintes génétiques* ont ajouté à la base de données cinq nouvelles catégories de profils génétiques, notamment l'ADN de personnes victimes de crime; de donneurs volontaires; de personnes disparues et de leurs parents. Au moment de la rédaction du présent rapport, ces modifications n'étaient pas encore en vigueur.

La création de la banque de données remonte à 2000, mais la Gendarmerie royale du Canada (GRC) n'a présenté aucune EFVP à cet égard avant 2014, principalement parce que les exigences fédérales en matière d'EFVP n'ont été mises en œuvre qu'en 2002, soit après la création de la banque de données. L'EFVP ne comportait aucune évaluation des nouveaux risques d'atteinte à la vie privée qui pourraient découler des nouvelles catégories de profils génétiques à ajouter à la banque de données. Nous nous attendons à ce que la GRC mène une nouvelle EFVP à cet égard et elle s'y est d'ailleurs engagée.

Gendarmerie royale du Canada — Centre national pour les personnes disparues et restes non identifiés

La GRC a présenté une EFVP sur le Centre national pour les personnes disparues et restes non identifiés. Ce centre offre aux agents chargés de l'application de la loi, aux médecins légistes et aux coroners en chef partout au Canada des services spécialisés à l'appui des enquêtes sur les personnes disparues et les restes non identifiés.

Les modifications susmentionnées à la *Loi sur l'identification par les empreintes génétiques* ont également élargi le mandat du centre en créant de nouveaux fichiers de profils génétiques des personnes disparues et de leurs parents ainsi que des restes humains. Cette information est accessible dans le cadre des enquêtes.

Le Commissariat a formulé plusieurs recommandations à la GRC concernant le fonctionnement du centre en ce qui a trait aux mesures de sécurité et à la limitation de la communication des renseignements personnels. Nous nous attendons à ce que la GRC effectue une nouvelle EFVP pour évaluer tout nouveau risque d'atteinte à la vie privée associé à l'expansion du centre. Elle en a d'ailleurs pris l'engagement.

Nous continuerons de suivre de près cette initiative et celle de la Banque nationale de données génétiques.

Utilisation accrue de l'information des médias sociaux et de sources ouvertes

En 2014-2015, nous avons reçu des EFVP ou avons été consultés relativement à plusieurs initiatives fédérales utilisant ou prévoyant d'utiliser de l'information « de sources ouvertes » ou « accessible au public ». Dans certains cas, il s'agirait notamment de renseignements personnels recueillis sur des sites de médias sociaux comme Facebook et Twitter.

Les Services de base de données sur l'intégrité de Travaux publics et Services gouvernementaux Canada (TPSGC) figurent parmi les initiatives qui proposent de recueillir et d'utiliser ce type d'information. Ils fournissent aux responsables des marchés publics des renseignements généraux sur les entreprises qui soumissionnent pour les contrats. Emploi et Développement social Canada envisage d'utiliser ce type d'information pour évaluer le degré de satisfaction à l'égard des services gouvernementaux, comme les demandes de passeport et les services d'emploi.

Nous avons notamment conseillé à TPSGC de faire attention à la possibilité que cette information soit périmée, hors de son contexte ou inexacte. Nous avons aussi soulevé la question du consentement, car les personnes qui formulent des commentaires dans les médias sociaux ne peuvent

raisonnablement s'attendre à ce que les représentants du gouvernement recueillent et utilisent cette information.

En réponse à nos recommandations et après avoir apporté certaines modifications à la conception du programme, TPSGC nous a informés qu'il s'en tiendrait dorénavant à l'information digne de confiance provenant de sources authentifiées, par exemple des rapports judiciaires, et qu'il ne recueillerait pas d'information de « sources ouvertes ». Dans le cas d'Emploi et Développement social Canada, nous devrions recevoir une EFVP sur la collecte de renseignements personnels sur les sites de médias sociaux pour évaluer le degré de satisfaction du public à l'égard des services gouvernementaux si ce type de projet va de l'avant.

Enquêtes

En 2014-2015, le Commissariat a mené à bien 1 239[5] enquêtes, en légère hausse par rapport aux 1 214[6] enquêtes de l'exercice précédent. Le nombre de dossiers fermés est demeuré stable, mais le nombre de plaintes reçues a monté en flèche pour atteindre 3 977, de loin le nombre le plus élevé jamais enregistré. Il s'agit d'une augmentation de 124 % par rapport à l'exercice précédent.

Toutefois, cette hausse est attribuable en grande partie à quelques personnes ayant déposé des plaintes multiples. Sur près de 4 000 plaintes reçues en 2014-2015, on en comptait 3 154 déposées par quelques personnes qui avaient présenté huit plaintes ou plus chacune — dans certains cas, plusieurs centaines. Si l'on fait abstraction de ces cas, le Commissariat a accepté 1 040 plaintes au cours du dernier exercice, soit un nombre similaire à celui de 2013-2014.

Pour gérer le risque que le traitement de ces dossiers empêche d'autres personnes d'avoir accès à ses services, le Commissariat a adopté une stratégie à l'égard des plaintes multiples.

5 Le nombre d'enquêtes est inférieur au nombre de plaintes, car nous avons exclu deux cas où une enquête a permis de fermer plusieurs dossiers de plaintes multiples se rapportant à deux incidents distincts (atteinte à la sécurité des données touchant les participants au Programme d'accès à la marihuana à des fins médicales de Santé Canada et perte d'une clé USB mettant en cause Emploi et Développement social Canada et Justice Canada), qui ont totalisé 668 dossiers de plaintes fermés.

6 Sans compter les 871 plaintes associées à l'enquête sur la perte d'un disque dur à Emploi et Développement social Canada.

Ainsi, nous nous efforçons d'offrir nos services aux personnes ayant déposé plusieurs plaintes au cours d'une courte période pour accorder la priorité à leur dossier — nous ouvrons les enquêtes sur les plaintes les plus importantes déposées par ces personnes mais, dans certains cas, nous reportons les autres jusqu'à ce que les premières enquêtes aient été menées à bien. Grâce à cette approche, le Commissariat peut arriver à un meilleur équilibre entre les besoins de tous les plaignants et assurer un traitement rapide et équitable de l'ensemble des plaintes.

Comme le nombre de plaintes et leur complexité ne cessent d'augmenter, le Commissariat continue à explorer des moyens de moderniser ses enquêtes et d'en améliorer l'efficacité. Le processus de règlement rapide permet de fermer davantage de dossiers (hausse de 22 % par rapport à 2013-2014). Nous avons aussi effectué un examen pour déterminer s'il était possible d'apporter des améliorations supplémentaires afin de réduire le délai de traitement des plaintes.

Il est essentiel d'accroître l'efficacité pour tirer le maximum de nos ressources limitées, mais nous n'en demeurons pas moins déterminés à maintenir un niveau d'excellence élevé dans les enquêtes.

Les dossiers résumés ci-après illustrent certains moyens par lesquels nos enquêtes révèlent des lacunes importantes dans la protection des renseignements personnels et aident à protéger le droit des Canadiens à la vie privée en mettant l'accent sur les enjeux associés aux relations employés-employeur et aux processus administratifs.

Pour lire la version intégrale de chaque rapport de conclusions résumé ci-dessous, allez à : https://www.priv.gc.a/cf-dc/pa/index1415_e.asp

Vidéosurveillance des employés et droit à la vie privée — un équilibre fragile

Un employé de l'Agence des services frontaliers du Canada (ASFC) alléguait que les douzaines de caméras en place à un poste frontalier entre le Canada et les États-Unis servaient non seulement à assurer la sécurité, mais aussi à surveiller la conduite et le rendement des employés.

Selon la politique de l'Agence sur l'utilisation ouverte de techniques de surveillance et d'enregistrement audio et vidéo, la vidéosurveillance peut être utilisée non seulement à des fins de surveillance, mais aussi pour aider à assurer l'intégrité des programmes et l'assurance qualité. La politique précise qu'il pourrait notamment s'agir de surveiller les interactions entre les employés de l'organisme et le public, d'assurer l'efficacité et de rassembler l'information voulue pour faire la preuve d'allégations de mauvaise conduite

ou d'activité illégale mettant en cause du personnel.

Le Commissariat reconnaît que l'ASFC, en sa qualité d'organisme manifestement chargé de l'application de la loi, doit maintenir un niveau élevé de crédibilité et de confiance du public afin de mettre en œuvre ses programmes efficacement. Pour remplir son mandat, l'Agence doit s'assurer que les employés se conforment aux codes de conduite, mais cela ne signifie pas pour autant que son affirmation selon laquelle ces utilisations de la vidéosurveillance et d'autres utilisations énoncées dans sa politique sont conformes à la *Loi sur la protection des renseignements personnels*.

De nombreux comportements des employés peuvent relever du champ de l'« assurance qualité », y compris l'utilisation d'une caméra vidéo pour observer leur rendement, par exemple pour voir le nombre de voyageurs qu'un agent accueille en une heure.

De par sa nature même, la vidéosurveillance est intrusive. Elle permet de recueillir toutes sortes de renseignements personnels, dont une très petite portion peut avoir un lien avec la raison à l'origine de la mise en place des caméras.

Dans ce dossier, nous avons jugé que l'Agence n'avait pas fait la preuve qu'il était nécessaire de recueillir les renseignements personnels des employés pour toute la gamme de fins citées comme étant associées à l'intégrité des programmes, ce qui contrevient à l'article 4 de la Loi, en vertu duquel « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ».

L'ASFC a mis à jour sa politique pour indiquer clairement comment elle a l'intention d'utiliser la vidéosurveillance et précisé qu'elle ne s'en servira pas pour observer le rendement des employés. Elle s'est aussi engagée à nous fournir des scénarios actualisés pour orienter les employés dans la mise en œuvre de la politique. Jusqu'à ce que nous ayons reçu les scénarios dans le cadre de notre suivi prévu un an après la clôture de l'enquête, et obtenu la certitude qu'ils concordent avec l'approche énoncée dans la politique mise à jour, nous considéreons cette plainte comme fondée et conditionnellement résolue[7].

Insigne nominatif tout à fait légitime pour les agents des services frontaliers

À la suite de la décision de l'ASFC d'obliger ses agents à porter sur leur uniforme un insigne indiquant leur nom de famille, 43 agents ont déposé une plainte alléguant qu'il s'agissait d'une utilisation et d'une communication

7 L'enquête a corroboré les allégations et l'institution s'est engagée à mettre en œuvre les recommandations formulées par le Commissariat. L'institution doit maintenant faire la preuve qu'elle les a mises en œuvre dans les délais prévus.

inappropriées de leurs renseignements personnels.

Les plaignants alléguaient qu'ils seraient plus vulnérables au harcèlement et à l'intimidation exercés par les voyageurs mécontents du fait qu'on les identifierait par leur nom plutôt que par un numéro. L'Agence a fait valoir que sa politique concorde avec celle de ses partenaires, notamment la Gendarmerie royale du Canada, les Forces armées canadiennes, le Service correctionnel du Canada et la Customs and Border Protection des États-Unis — toutes des institutions où les agents de première ligne portent un insigne nominatif.

Nous avons jugé que le nom de famille affiché sur l'insigne des employés de première ligne de l'ASFC constitue une exception à la définition de « renseignements personnels », ce qui permet essentiellement l'utilisation et la communication d'information révélant qu'une personne est ou a été un agent ou un employé d'une institution gouvernementale. La finalité sous-jacente de cette exception consiste à s'assurer que l'État et ses agents rendent compte de leurs actes au public. En conséquence, nous avons jugé que les plaintes étaient non fondées.

Atteinte à la sécurité de données découlant d'une violation du principe du « besoin de savoir »

Dans ce dossier, le plaignant a attiré notre attention sur un article paru dans *La Presse.* Cet article rapportait qu'Affaires autochtones et Développement du Nord Canada (AADNC) avait produit un document citant le nom des personnes qui avaient présenté, en vertu de la *Loi sur l'accès à l'information,* des demandes concernant les dépenses d'un ancien ministre. Il nommait l'un des demandeurs et précisait que le document avait été communiqué à des employés d'AADNC ne faisant pas partie de la Division de l'accès à l'information et de la protection des renseignements personnels du ministère.

Affaires autochtones et Développement du Nord Canada a déclaré au Commissariat l'atteinte à la sécurité des données le jour même et lui a fourni une liste des personnes au sein du ministère qui avaient obtenu copie du document en question. Le nom de fonctionnaires des Finances et services des marchés, l Planification et gestion des ressources et des Communications figurait sur la liste.

En vertu de la *Loi sur la protection des renseignements personnels*, les renseignements personnels recueillis ne peuvent servir à une organisation qu'aux fins auxquelles ils ont été recueillis. Dans ce cas, les renseignements personnels des intéressés avaient été recueillis à la seule fin de s'assurer que la Division de l'accès à l'information et de la protection des renseignements personnels sache où envoyer la réponse à leur demande. En communiquant cette information à des personnes de l'extérieur de la Division, AADNC a contrevenu à la *Loi sur la protection des renseignements personnels.*

En outre, une enquête d'AADNC a permis de retracer le document obtenu par *La Presse*. Il s'agissait d'une copie faite pour un fonctionnaire de l'extérieur de la Division. Dans ce cas, AADNC a aussi contrevenu à la *Politique sur l'accès à l'information* du président du Conseil du Trésor, selon laquelle il faut veiller à ce que l'identité des requérants soit protégée et à ce qu'elle ne soit divulguée qu'aux personnes ayant un réal « besoin de savoir » dans l'exercice de leurs fonctions relatives à un programme ou à une activité légitime.

Nous avons recommandé à AADNC d'examiner ses politiques et procédures pour le traitement des demandes de la Division de l'accès de l'information et de la protection des renseignements personnels. Nous lui avons aussi demandé de nous dans un délai de six mois informer des mesures prises pour assurer le respect du principe du besoin de savoir. Depuis, le ministère a donné suite à notre demande et nous sommes satisfaits des mesures prises pour éviter qu'un incident similaire se reproduise.

Communication de renseignements sur la santé dépassant les objectifs de la Loi sur l'emploi dans la fonction publique

Le Commissariat a ouvert une enquête sur la Commission de la fonction publique du Canada (CFP). Il ressort de cette enquête que, même si la *Loi sur la protection des renseignements personnels* permette de communiquer des renseignements personnels sans le consentement de l'intéressé dans certaines situations, cette communication doit se limiter à l'information absolument nécessaire.

Au cours d'une enquête menée par la CFP sur des allégations de fraude dans un processus de nomination, un enquêteur de la CFP a interrogé la personne qui avait déposé une plainte auprès du Commissariat (laquelle faisait l'objet de l'enquête de la CFP) et quatre autres personnes. La plaignante avait remis à l'enquêteur une lettre de son médecin renfermant des détails sur son état de santé au moment de l'incident allégué.

Après les interrogatoires, l'enquêteur de la CFP a produit un rapport dans lequel figurait la lettre du médecin. Il en a remis une copie à la plaignante et à chacun des quatre témoins. D'après la Commission, cette pratique est conforme à son guide à l'intention des enquêteurs, selon lequel l'enquêteur doit, avant de préparer son rapport final, donner aux personnes susceptibles d'être touchées par l'enquête une chance de formuler leurs commentaires.

Nous avons toutefois constaté que le guide indique aussi que si une personne est touchée uniquement par une petite partie du rapport factuel, l'enquêteur peut décider qu'il faut lui communiquer uniquement la partie en question.

À notre avis, l'enquêteur de la CFP aurait dû exercer davantage son pouvoir discrétionnaire au moment de déterminer quels renseignements se trouvant dans le rapport factuel devaient être communiqués aux témoins. Nous avons donc conclu que la CFP avait communiqué des renseignements personnels sans le consentement de l'intéressée, contrevenant ainsi à la *Loi sur la protection des renseignements personnels,* et que la plainte était fondée.

La CFP s'est engagée à améliorer ses procédures pour assurer la conformité à la *Loi sur la protection des renseignements personnels* au moment de communiquer des renseignements personnels. Elle s'attachera particulièrement à appliquer le principe du « besoin de savoir » afin de déterminer la quantité d'information dans ses rapports qui doit être communiquée. Le Commissariat fera le suivi auprès de la CFP au cours de l'exercice à venir pour s'assurer qu'elle a mis en œuvre toutes les modifications proposées à son processus d'enquête et qu'elle respecte les obligations lui incombant en vertu de la *Loi sur la protection des renseignements personnels*.

Une plainte concernant le registre des armes d'épaule sans recours à la suite de l'abrogation rétroactive de dispositions de la Loi sur la protection des renseignements personnels

Selon les allégations du plaignant, la Gendarmerie royale du Canada (GRC) avait utilisé des renseignements personnels tirés du registre des armes d'épaule, maintenant abrogé, pour localiser et saisir des armes enregistrées dans des habitations évacuées en raison des inondations dans la région de High River, en Alberta, en juin 2013.

D'après le plaignant, on entendait dans un enregistrement vidéo montrant des segments d'activités d'intervention d'urgence un membre de la GRC affirmer qu'il avait « localisé toutes les armes à feu ». Le plaignant a affirmé que le membre connaissait donc le nombre exact d'armes dans une maison en particulier — *renseignement que seul l'accès à l'information stockée dans le registre aurait permis d'obtenir*.

Toute l'information figurant dans le registre aurait dû être détruite après l'adoption de la *Loi sur l'abolition du registre des armes d'épaule* en avril 2012. La GRC a affirmé que toute l'information avait bel et bien été détruite dès la fin d'octobre 2012. Nous avons fait enquête pour déterminer si elle continuait d'utiliser des renseignements personnels tirés du registre, par exemple, des copies de ce registre, après sa destruction présumée et, en particulier, si elle avait utilisé cette information dans le cadre de l'incident de High River.

Dans les observations qu'elle a formulées au cours de notre enquête, la GRC a fait valoir que le registre proprement dit avait été détruit en octobre 2012 et qu'aucun détachement de la GRC, y compris celui de High River, n'en avait gardé copie. Soulignons que la GRC a indiqué

que des renseignements personnels tirés du registre d'armes d'épaule et utilisés avant l'adoption de la *Loi sur l'abolition du registre des armes d'épaule* auraient pu dans certains cas être conservés, par exemple dans des cahiers de notes, des dossiers d'enquête ou d'autres fichiers connexes. De plus, l'utilisation de ces renseignements personnels dans le contexte d'une enquête opérationnelle serait conforme à la fin à laquelle ils ont été compilés. La GRC n'a toutefois pas donné plus de détails.

Nous n'avons pu examiner ce cas de façon plus approfondie. En effet, vers la fin de notre enquête, le Parlement a adopté le projet de loi C59, qui apportait à la *Loi sur l'abolition du registre des armes d'épaule* des modifications en vertu desquelles la *Loi sur la protection des renseignements personnels* ne s'applique pas aux fichiers relatifs à l'enregistrement des armes à feu ni aux copies de ces fichiers. Ces dispositions s'appliquaient rétroactivement à compter d'octobre 2011. À la lumière de l'information recueillie à cette date, nous n'avons pu conclure que la GRC avait contrevenu à la *Loi sur la protection des renseignements personnels*.

L'abrogation rétroactive des protections assurées par la *Loi sur la protection des renseignements personnels* constitue une première. Dans un Mémoire présenté au Comité sénatorial permanent des finances nationales sur le projet de loi C59 en juin 2015, le commissaire Therrien a souligné l'importance de permettre aux individus de contester la manière dont le gouvernement utilise leurs renseignements personnels.

Collecte de renseignements non nécessaires sur la santé d'un membre de la GRC

La plaignante, membre de la Gendarmerie royale du Canada (GRC), alléguait que l'organisation avait recueilli sans son consentement en 2003 des renseignements sur sa santé et sa situation financière.

Elle avait demandé à Anciens Combattants Canada (ACC) une pension d'invalidité, que le ministère accorde et administre au nom de la GRC en vertu d'un protocole d'entente conclu entre les deux organisations. ACC a par la suite envoyé à la plaignante une lettre indiquant qu'il lui avait accordé une pension d'invalidité. Il en a envoyé copie au Centre national des politiques en rémunération de la GRC et une autre copie a été déposée à la direction chargée des servcies de santé nationaux de la GRC. Or, la lettre renfermait des renseignements sur la santé de la plaignante ainsi que le montant de l'indemnité qu'elle toucherait.

À notre avis, le Centre national des politiques en rémunération, qui fait partie du Service divisionnaire des ressources humaines de la GRC, n'a pas besoin des renseignements personnels sur la santé de la plaignante pour administrer sa pension — pas plus que la direction chargée des servcies de santé nationaux n'a besoin des renseignements sur sa situation financière pour lui fournir des

services de santé. Nous avons jugé qu'il y avait eu contravention à l'article 4 de la *Loi sur la protection des renseignements personnels*, selon lequel les renseignements personnels recueillis par une institution gouvernementale doivent avoir un lien direct avec ses programmes ou ses activités. En conséquence, nous avons conclu que la plainte était fondée.

Au cours de notre enquête portant sur cette plainte, on nous a présenté des données probantes montrant que la GRC et ACC avaient convenu en 2005 — à la demande de la GRC — qu'ACC cesserait d'envoyer au Centre national des politiques en rémunération de la GRC les renseignements sur la santé des demandeurs de pension d'invalidité. Malgré le protocole d'entente conclu entre les deux organisations, ACC a continué d'envoyer ces renseignements personnels au Centre et celui-ci a continué de les recueillir. C'est seulement en 2010 qu'ACC a mis fin à cette pratique.

Nous avons vivement recommandé de mettre à jour ce protocole d'entente pour donner une orientation détaillée sur la transmission appropriée de ce type de renseignements personnels de nature délicate entre les deux institutions. Nous ferons le suivi auprès de la GRC après un an pour vérifier si le protocole a été mis à jour comme demandé.

Enregistrement réputé « temporaire » détruit prématurément

Le plaignant a été congédié par le ministère de la Défense nationale (MDN) après une audience à l'issue de laquelle on avait recommandé de mettre fin à sa participation à un programme de formation des Forces armées canadiennes. Il a fait appel de la décision et demandé au MDN une copie de l'enregistrement audio de l'audience à laquelle il avait pris part. Le ministère l'a alors informé que l'enregistrement avait été effacé.

Selon les allégations du plaignant, le MDN avait contrevenu au paragraphe 6(1) de la *Loi sur la protection des renseignements personnels,* en vertu duquel une institution fédérale doit conserver pendant au moins deux ans après leur dernière utilisation les renseignements qu'elle a utilisés à des fins administratives, à moins que la personne à qui ils se rapportent consente à leur retrait. Cette disposition vise à permettre à l'individu concerné d'exercer son droit d'accès à ces renseignements.

Le MDN a fait valoir qu'il s'agissait d'un enregistrement « temporaire » utilisé uniquement par le secrétaire du Comité d'évaluation des progrès pour rédiger le compte rendu d'audience, qui constitue le compte rendu « officiel » des délibérations. Le plaignant soutenait que le compte rendu était inexact et incomplet et que, en l'absence de l'enregistrement, il était incapable d'étayer son allégation.

Il fallait déterminer si l'enregistrement audio de l'audience était assujetti aux exigences

en matière de conservation énoncées dans la *Loi sur la protection des renseignements personnels*, dans laquelle le terme « temporaire » ne figure pas. Dans ce dossier, personne ne conteste le fait que l'enregistrement audio contenait les renseignements personnels du plaignant et avait été utilisé à des fins administratives, à savoir pour déterminer son avenir dans le programme de formation. En conséquence, l'enregistrement était assujetti aux dispositions de la Loi relatives à la conservation des renseignements personnels et nous avons conclu que la plainte était fondée.

Au cours de cette enquête, nous avons appris que le MDN conservait l'enregistrement audio de certaines audiences et en retirait d'autres, sans aucune justification apparente. Nous avons encouragé le ministère à élaborer et à appliquer des procédures concernant la collecte d'information dans le cadre des audiences du Comité d'évaluation des progrès, ainsi que la conservation et le retrait de cette information et, entre-temps, à conserver pendant au moins deux ans les enregistrements ou leur transcription mot à mot, à moins que l'intéressé ait consenti à leur destruction avant l'expiration de ce délai.

RÈGLEMENT RAPIDE

La proportion des plaintes traitées par voie de négociation ou de conciliation à la satisfaction des parties a augmenté en 2014-2015. Dans l'ensemble, le processus de règlement rapide a permis de fermer 422 dossiers,

LE RÈGLEMENT RAPIDE À L'ŒUVRE

Plainte pour communication non autorisée déposée contre le Service correctionnel du Canada

Dans ce dossier, le plaignant alléguait que dans un pénitencier de la Saskatchewan, toute la correspondance personnelle sortante et tous les formulaires de demande renfermant des renseignements protégés étaient placés dans un plateau non sécurisé accessible à toute personne se trouvant dans l'aire de réception. Après le dépôt de la plainte et les demandes d'information connexes présentées par le Commissariat, le Service correctionnel du Canada remplacé le plateau par un coffret verrouillé pour répondre aux préoccupations concernant la protection des renseignements personnels. La plainte a donc été résolue.

Plainte pour refus d'accès contre le ministère des Affaires étrangères, du Commerce et du Développement

Un individu alléguait que des documents manquaient dans la réponse qu'il avait reçue à la suite de sa demande d'accès à ses renseignements personnels adressée au ministère des Affaires étrangères, du Commerce et du Développement. Le Commissariat a contacté le ministère, qui a alors effectué une autre recherche et trouvé les documents en question, qu'il a remis au plaignant. La plainte a donc été résolue.

comparativement à 345 au cours de l'exercice précédent. Malgré une légère augmentation du délai moyen de règlement des plaintes selon ce processus — qui est passé de 2,11 mois en 2013-2014 à 3,24 mois au cours de l'exercice écoulé —, cette méthode joue de toute évidence le rôle escompté en réduisant le nombre d'enquêtes régulières.

Trente-quatre pour cent (34 %) des dossiers de plaintes fermés en 2014-2015 l'ont été au moyen du processus de règlement rapidement. Fait à signaler, près de 60 % des plaintes (101 sur 176) portant sur l'accès aux renseignements personnels déposées contre le Service correctionnel du Canada au cours de l'exercice ont été résolues au moyen du processus de règlement rapide. Ce résultat exceptionnel montre que toutes les parties sont manifestement déterminées à résoudre leurs différends d'une manière plus efficiente et efficace.

AMÉLIORATION DES DÉLAIS DE TRAITEMENT

En vertu de la *Loi sur la protection des renseignements personnels*, les institutions fédérales doivent répondre dans les 30 jours aux demandes de communication de renseignements personnels présentées par des personnes. Dans certaines situations, elles peuvent demander une prorogation de 30 jours.

Le nombre de plaintes déposées contre les institutions qui ne respectent pas le délai prévu a été élevé au cours de chacun des derniers exercices. En 2014-2015, il a atteint un sommet de 2 612 —un nombre plus de quatre fois supérieur à celui de l'exercice précédent —, mais cette forte augmentation est attribuable aux plaintes multiples déposées par quelques personnes. En fait, si l'on fait abstraction des plaintes multiples, le nombre de plaintes relatives au non-respect des délais prévus par la loi a diminué par rapport à l'exercice précédent (377 comparativement à 585), notamment en raison d'une réduction de 35 % du nombre de plaintes de ce type déposées contre le Service correctionnel du Canada.

Le Commissariat continue de travailler en collaboration avec les institutions, comme le Service correctionnel du Canada, pour régler les problèmes de délais, notamment en demandant des plans d'action et des dates d'engagement pour la production des renseignements personnels demandés par une personne. À l'avenir, il poursuivra ses efforts et suivra de près l'évolution de la situation afin de déterminer si la situation observée en 2014-2015 constitue un phénomène ponctuel ou si elle marque le début d'une tendance plus vaste.

Vérifications

En vertu de la *Loi sur la protection des renseignements personnels,* le commissaire peut examiner les pratiques des institutions fédérales en matière de protection de la vie privée et recommander des mesures correctives au besoin. La Loi ne lui confère pas de pouvoirs en matière d'application, mais le commissaire peut publier ses conclusions et recommandations. En outre, le Commissariat fait généralement un suivi auprès des institutions vérifiées deux ans après la publication du rapport de vérification initial et demande alors quelles mesures elles ont prises pour donner suite à ses recommandations.

Résultats du suivi auprès d'Anciens Combattants Canada

En 2014-2015, nous avons fait le suivi de notre vérification de 2012 portant sur les pratiques de traitement des renseignements personnels en vigueur à Anciens Combattants Canada (ACC). Dans sa réponse, le ministère a déclaré avoir mis en œuvre les 13 recommandations formulées dans notre rapport de vérification. ACC a par exemple mis en place pour son principal Réseau de prestation des services aux clients, un système qui fait en sorte que seuls les employés ayant un « besoin de savoir » ont accès aux renseignements personnels sur la santé d'un client et à leurs autres renseignements personnels de nature délicate.

ACC s'est aussi doté d'un processus d'élimination des documents pour s'assurer que les renseignements personnels recueillis sur le Réseau ne sont pas conservés plus longtemps que nécessaire. Il a en outre créé une nouvelle fonction afin que les employés consignent et confirment dans le Réseau la réception du consentement des clients. Cette mesure aidera le ministère à s'assurer que ses clients sont informés de la façon dont leurs renseignements pourraient être recueillis, utilisés et communiqués et des raisons pour lesquelles ils le sont, qu'ils comprennent ce qui en est et qu'ils donnent leur consentement.

Suivi à venir de la vérification de l'Agence du revenu du Canada effectuée en 2013

Comme nous l'avons signalé au chapitre 4, nous avons vérifié en 2013 les pratiques de traitement des renseignements personnels en vigueur à l'Agence du revenu du Canada. Nous ferons à l'hiver 2016 le suivi des mesures prises par l'Agence en réponse aux recommandations que nous avions formulées à l'issue de notre vérification.

Publication du rapport de vérification sur les dispositifs de stockage portables

Comme l'explique le commissaire dans son message, les nombreuses atteintes substantielles à la sécurité des données survenues au cours des dernières années, qui mettaient en cause des dispositifs de stockage portables comme des clés USB et des disques durs portables, ont incité le Commissariat à entreprendre en 2014 une vérification de la gestion de ces dispositifs au sein des institutions fédérales. On trouvera plus de détails à ce sujet au chapitre 4.

Nouvelle vérification — Emploi et Développement social Canada et Services partagés Canada

Le Commissariat a entrepris en février 2015 une vérification des pratiques de traitement des renseignements personnels en vigueur à Emploi et Développement social Canada et à Services partagés Canada. Cette vérification met l'accent sur certains aspects des risques d'atteinte à la vie privée dans le cadre du Programme de la sécurité de la vieillesse. Nous devrions la terminer et publier un rapport en 2016.

Communication pour des raisons d'intérêt public, notamment en vertu de l'alinéa 8(2)*m*)

L'alinéa 8(2)*m*) de la *Loi sur la protection des renseignements personnels* autorise une institution à communiquer des renseignements personnels sans le consentement de l'individu qu'ils concernent dans les cas où, de l'avis du responsable de l'institution :

- des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée; ou
- l'individu concerné en tirerait un avantage certain.

Toute institution qui a l'intention de communiquer des renseignements personnels en vertu de cette disposition doit dans la mesure du possible donner un préavis écrit de la communication au Commissariat ou l'aviser par écrit immédiatement après la communication.

Sur réception de l'avis de communication, le Commissariat examine la communication. Il peut faire part de ses préoccupations à l'institution ou lui recommander de mettre l'intéressé au courant de la communication si elle ne l'a pas déjà fait. Si l'institution refuse de mettre au courant l'individu concerné, le commissaire est habilité à le faire. Toutefois, la décision de diffuser des renseignements personnels pour des raisons d'intérêt public revient uniquement au responsable de l'institution. Le commissaire n'a pas le pouvoir d'en empêcher la communication.

En 2014-2015, nous avons traité 266 avis de communication reçus en vertu de

l'alinéa 8(2)*m*) de la *Loi sur la protection des renseignements personnels* ou de dispositions similaires figurant dans d'autres lois fédérales. Il s'agit d'un volume comparable au nombre d'avis reçus au cours de l'exercice précédent. Toutefois, en 2013-2014, le Commissariat en avait reçu 300 % de plus qu'au cours des deux exercices précédents. Cette augmentation est attribuable en grande partie à une diligence accrue de certaines institutions en matière de déclaration. Emploi et Développement social Canada, en particulier, a pris l'habitude de déclarer les communications faites à la police dans les cas où ses propres clients s'exposaient eux-mêmes ou exposaient d'autres personnes à un préjudice grave.

Activités de sensibilisation

Ateliers sur les évaluations des facteurs relatifs à la vie privée

Le Commissariat a continué d'offrir des ateliers à l'intention des institutions fédérales désireuses de renforcer leur capacité à effectuer et à lui présenter des évaluations des facteurs relatifs à la vie privée (EFVP) rigoureuses et efficaces. En réponse aux commentaires formulés par les institutions au cours de l'exercice précédent, nous avons légèrement modifié notre approche pour privilégier les déjeuners-causeries en plus petits groupes favorisant les échanges. Nous avons organisé des séances qui ciblaient différents auditoires; certaines comprennent une introduction et un aperçu du processus d'EFVP et d'autres portaient sur des aspects couvrant des sujets plus complexes, comme les risques d'atteinte à la vie privée associés à la technologie.

Nous avons reçu des commentaires très positifs et nous prévoyons de continuer à offrir de telles séances en utilisant différents formats et en couvrant des sujets variés en fonction des besoins des participants.

À quoi s'attendre quand on dépose une plainte

Vers la fin de 2014-2015, nous avons affiché sur notre site Web un guide qui aidera les Canadiens à comprendre le mode de fonctionnement du processus de plaintes en vertu de la *Loi sur la protection des renseignements personnels*.

Ce nouveau guide, intitulé *À quoi s'attendre au cours d'une enquête sur une plainte en vertu de la* Loi sur la protection des renseignements personnels, fait appel à une série de questions et réponses pour couvrir les notions élémentaires, depuis les organisations assujetties à la *Loi sur la protection des renseignements personnels* jusqu'au fonctionnement de notre processus de règlement rapide. Il aidera aussi les organisations à mieux comprendre le processus d'enquête du Commissariat et ses attentes dans le cadre d'une enquête.

Discours, présentations et outils d'information

Le commissaire Therrien a pris la parole devant des professionnels de la protection de la vie privée travaillant dans le secteur public, dans le cadre de la Conférence de l'Association canadienne d'accès à l'information et de protection des renseignements personnels et de la Réunion de la collectivité de l'accès à l'information et de la protection des renseignements personnels, qui ont eu lieu en décembre.

En parallèle, le Commissariat s'attache activement à sensibiliser le secteur public. Ainsi, il a notamment pris part au Symposium annuel 2014 de l'Association professionnelle des cadres supérieurs de la fonction publique du Canada (APEX), activité à laquelle les cadres supérieurs de la fonction publique fédérale participent en grand nombre.

Des représentants du Commissariat ont aussi donné plusieurs présentations à des fonctionnaires fédéraux en 2014-2015, par exemple sur :

- la circulation transfrontière de données — au cours d'un atelier s'adressant à la communauté de pratique de la biométrie organisé par Recherche et développement pour la défense Canada;
- la protection des renseignements personnels dans le contexte des ressources humaines — au cours d'une réunion de professionnels en ressources humaines organisée par le Conseil RH;
- la protection de la vie privée et la confidentialité dans le domaine de la recherche sur la santé sous réglementation fédérale — devant le Comité d'éthique de la recherche de Santé Canada.

Annexe 1 – Définitions

GRANDS TYPES DE PLAINTES

1. Accès

Accès — Les renseignements personnels n'auraient pas tous été communiqués, soit parce qu'il manque des documents ou des renseignements, soit parce que l'institution a invoqué des exceptions afin de ne pas communiquer des renseignements.

Correction ou annotation — L'institution n'aurait pas apporté les corrections aux renseignements personnels ou ne les aurait pas annotés parce qu'elle n'approuve pas les corrections demandées.

Langue — Les renseignements personnels n'auraient pas été fournis dans la langue officielle du choix du demandeur.

Frais — Des frais auraient été exigés pour répondre à une demande de renseignements en vertu de la *Loi sur la protection des renseignements personnels*; aucuns frais ne sont actuellement imposés u pour l'obtention de renseignements personnels.

Répertoire — *Info Source* (répertoire du gouvernement fédéral qui décrit chaque institution et les banques de données — groupes de fichiers sur un même sujet — que l'institution possède) ne décrirait pas de façon adéquate le fonds de renseignements personnels d'une institution.

2. Protection des renseignements personnels

Exactitude — L'institution n'aurait pas pris toutes les mesures raisonnables pour s'assurer que les renseignements personnels utilisés à des fins administratives sont aussi exacts, à jour et complets que possible.

Collecte — L'institution aurait recueilli des renseignements personnels qui ne sont pas nécessaires à l'un de ses programmes ou à l'une de ses activités; les renseignements personnels n'auraient pas été recueillis directement auprès de la personne concernée; ou la personne n'aurait pas été informée des fins auxquelles les renseignements personnels ont été recueillis.

Conservation et retrait — Des renseignements personnels n'auraient pas été conservés selon les calendriers de conservation et de retrait approuvés par les Archives nationales et publiés dans *Info Source :* ils auraient été détruits trop rapidement ou conservés trop longtemps.

En outre, les renseignements personnels utilisés à des fins administratives doivent être conservés pendant au moins deux ans après la dernière utilisation, à moins que la personne ait consenti à leur retrait.

Utilisation et communication — Des renseignements personnels auraient été utilisés ou communiqués sans le consentement de la personne concernée et ne satisferaient pas à l'un des critères d'utilisation ou de communication autorisée sans consentement énoncés aux articles 7 et 8 de la Loi.

3. Délais

Délais — L'institution n'aurait pas répondu dans les délais prescrits.

Avis de prorogation — L'institution n'aurait pas donné une justification appropriée pour la prorogation; elle aurait fait la demande de prorogation après le délai initial de 30 jours; ou elle aurait fixé l'échéance à plus de 60 jours de la date de réception de la demande.

Correction ou annotation — Délais — L'institution n'aurait pas corrigé les renseignements personnels ou n'aurait pas annoté le dossier dans les 30 jours suivant la réception d'une demande de correction.

CONCLUSIONS GÉNÉRALES ET AUTRES DÉCISIONS RENDUES EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

1. Conclusions d'enquêtes

Fondée — L'institution fédérale n'a pas respecté les droits d'une personne aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée et résolue — Les allégations ont été corroborées par l'enquête et l'institution gouvernementale a accepté de prendre des mesures correctives pour remédier à la situation.

Fondée et conditionnellement résolue — Les allégations ont été corroborées par l'enquête et l'institution s'est engagée à mettre en œuvre les recommandations formulées par le Commisariat et montré qu'elle l'avait fait dans les délais prévus.

Non fondée — L'enquête n'a pas permis de recueillir des données probantes afin de conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant en vertu de la *Loi sur la protection des renseignements personnels*, ou encore les données probantes recueillies étaient insuffisantes.

Résolue — Les données probantes recueillies au cours de l'enquête soutiennent les allégations soulevées dans la plainte, mais l'institution s'est engagé à prendre des mesures pour corriger le problème à la satisfaction du Commissariat.

Réglée — Le Commissariat a aidé à la négociation d'une solution satisfaisant toutes les parties dans le cadre de l'enquête, mais il n'a rendu aucune conclusion.

Abandonnée — L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. Un dossier peut être abandonné pour toutes sortes de raisons. Par exemple, il est possible que le plaignant ne veuille plus donner suite à à l'incident ou qu'on ne puisse pas le joindre afin d'obtenir des renseignements supplémentaires essentiels pour arriver à une conclusion.

Hors du champ d'application — À la lumière des renseignements préliminaires recueillis, le Commissariat a déterminé que la *Loi sur la protection des renseignements personnels* ne s'appliquait pas à l'institution ou à l'incident faisant l'objet de la plainte. Il n'a donc produit aucun rapport.

2. Autres décisions

Règlement rapide — Le dossier a été réglé avant même le début d'une enquête régulière. Par exemple, si une personne dépose une plainte concernant un incident qui a déjà fait l'objet d'une enquête par le Commissariat et que celui-ci l'a jugée conforme à la *Loi sur la protection des renseignements personnels*, la situation est expliquée au plaignant. Le Commissariat reçoit aussi parfois des plaintes pour lesquelles une enquête régulière aurait pu avoir des conséquences défavorables pour le plaignant. En pareil cas, on lui explique en détail la situation. Si le plaignant décide de ne pas aller de l'avant, la plainte est fermée à l'issue d'un processus de « règlement rapide ».

Annexe 2 — Tableaux statistiques

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* en 2014-2015

Catégorie	Total
Acceptées	
Accès	382
Délais	377
Protection des renseignements personnels	281
Total des plaintes acceptées et actives	**1 040**
Total des plaintes acceptées et en suspens*	2 937
Fermées à l'issue d'un processus de règlement rapide	
Accès	225
Délais	71
Protection des renseignements personnels	126
Total	**422**
Fermées à l'issue d'une enquête régulière	
Accès	225
Délais	409
Protection des renseignements personnels**	851
Total	**1 485**
Total des plaintes fermées	**1 907**
Atteintes déclarées	
Communication accidentelle	187
Vol	8
Perte	27
Accès non autorisé	34
Total des atteintes déclarées	**256**

* *Ces plaintes en suspens ont été déposées à titre individuel par quelques plaignants. Les 2 937 plaintes sont réparties comme suit : 690 avaient trait à l'accès, 2 236 aux délais et 11 à la protection des renseignements personnels.*

** *Comprend plusieurs séries de plaintes connexes ventilées comme suit : Emploi et Développement social Canada (164), Justice Canada (165) et Santé Canada (339).*

Violations de la *Loi sur la protection des renseignements personnels*, par institution

Intimé	Incident
Affaires autochtones et Développement du Nord Canada	9
Affaires étrangères, Commerce et Développement Canada	7
Agence canadienne d'évaluation environnementale	1
Agence du revenu du Canada	38
Agriculture et Agroalimentaire Canada	1
Anciens Combattants Canada	65
Bureau du Conseil privé	1
Centre de la sécurité des télécommunications	1
Citoyenneté et Immigration Canada	76
Commission canadienne des droits de la personne	1
Commission de la fonction publique du Canada	1
Conseil national de recherches Canada	1
Défense nationale	2
Emploi et Développement social Canada	4
Gendarmerie royale du Canada	5
Justice Canada	2
Patrimoine canadien	1
Pêches et Océans Canada	3
Ressources naturelles Canada	1
Secrétariat du Conseil du Trésor du Canada	1
Service correctionnel Canada	19
Service des poursuites pénales du Canada	2
Statistique Canada	3
Transports Canada	7
Tribunal des anciens combattants (révision et appel) Canada	4
Total	**256**

Délais de traitement des plaintes en vertu de la *Loi sur la protection des renseignements personnels* — Toutes les plaintes fermées, par décision

Type de plainte	Nombre de plaintes	Délai de traitement moyen (en mois)
Fondée*	406	7,06
Non fondée	189	13,66
Abandonnée	129	10,92
Fondée et résolue	40	19,14
Réglée	29	12,03
Résolue à l'issue d'une enquête régulière	24	13,13
Résolue au moyen du processus de règlement rapide	422	3,24
Total	**1 239**	**7,79**

* *Comprend une plainte représentative pour chacun des incidents et exclut les autres plaintes, dont le nombre est indiqué entre parenthèses : Emploi et Développement social Canada (164), Justice Canada (165) et Santé Canada (339).*

Délais de traitement des plaintes en vertu de la *Loi sur la protection des renseignements personnels* — Enquêtes régulières, par type de plainte

Type de plainte	Nombre de plaintes	Délai de traitement moyen (en mois)
Accès		
Accès	220	14,59
Correction ou annotation	3	7,44
Langue	2	10,05
Délais		
Délais	375	5,35
Avis de prorogation	34	4,02
Protection des renseignements personnels		
Utilisation et communication*	152	15,45
Collecte	22	18,26
Conservation et retrait	7	21,35
Exactitude	1	0,95
Autre	1	4,52
Total	**817**	**10,15**

* *Comprend une plainte représentative pour chacun des incidents et exclut les autres plaintes, dont le nombre est indiqué entre parenthèses : Emploi et Développement social Canada (164), Justice Canada (165) et Santé Canada (339).*

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 de plaintes	Délai de traitement moyen (en mois)
Accès		
Accès	222	2,78
Correction ou annotation	2	1,39
Langue	1	2,00
Délais		
Délais	70	2,01
Correction — Délais	1	7,25
Protection des renseignements personnels		
Utilisation et communication	99	5,24
Collecte	19	1,94
Conservation et retrait	6	3,98
Exactitude	2	9,48
Total	**422**	**3,24**

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 à l'issue d'une enquête régulière	Aban- donnée	Résolue au moyen du processus de règle-ment rapide	Réglée	Total
Administration canadienne de la sûreté du transport aérien	0	0	2					2
Affaires autochtones et Développement du Nord Canada	2	1		2	9	3		17
Affaires étrangères, Commerce et Développement Canada	0	0			1	1		2
Agence canadienne d'inspection des aliments	0	1				4		5
Développement économique Canada pour les régions du Québec	0	0		1				1
Agence de la santé publique du Canada	0	0	1		2			3
Agence des services frontaliers du Canada	1	7	48	1	7	23		87
Agence du revenu du Canada	0	5	9	8	5	22		49
Agriculture et Agroalimentaire Canada	0	0				1		1
Anciens Combattants Canada	4	1	8		2	3	1	19
Bureau de l'enquêteur correctionnel	0	1						1
Bureau du surintendant des institutions financières du Canada	0	0				1		1
Centre de la sécurité des télécommunications	0	0	1	0				1
Citoyenneté et Immigration Canada	1	1	4		3	8		17
Commissariat à l'information du Canada	0	1						1
Commissariat aux langues officielles	1	0						1
Commission canadienne des droits de la personne	0	0			1			1
Commission d'examen des plaintes concernant la police militaire	0	0	2					2
Commission de l'immigration et du statut de réfugié du Canada	0	0				1		1
Commission de la fonction publique du Canada	0	0	2			2		4
Commission des libérations conditionnelles du Canada	0	0	2			3		5
Conseil national de recherches Canada	0	0			1			1
Défense nationale	3	0	8	2	6	13	5	37
Emploi et Développement social Canada	170	1	1		8	38	1	219
Énergie atomique du Canada limitée	0	0				1		1

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 à l'issue d'une enquête régulière	Aban- donnée	Résolue au moyen du processus de règle-ment rapide	Réglée	Total
Environnement Canada	0	0				5		5
Financement agricole Canada	0	0			1	1		2
Gendarmerie royale du Canada	18	2	20	1	25	54	9	129
Industrie Canada	0	0				3		3
Justice Canada	167	1	2	1	6	8		185
Le service anglophone de la Société Radio-Canada	0	1				3		4
Monnaie royale canadienne	0	0				1		1
Office des eaux du Nunavut						1		1
Passeport Canada	0	0	1					1
Patrimoine canadien	1	0	1					2
Pêches et Océans Canada	0	0			3	3	2	8
Ressources naturelles Canada	0	0			2	1		3
Santé Canada	340	0	1	1	1	5	1	349
Secrétariat du Conseil du Trésor du Canada	0	0	1				1	2
Sécurité publique Canada	1	0						1
Service Canada	2	0	3	1	1	4		11
Service canadien du renseignement de sécurité	0	1	6	1		10		18
Service correctionnel Canada	9	11	26	4	16	101	9	176
Services partagés Canada	0	0				3		3
Société canadienne d'hypothèques et de logement	0	0				1		1
Société canadienne des postes	0	3	2			10		15
Statistique Canada	0	0	1			4		5
Transports Canada	1	0	2			1		4
Travaux publics et Services gouvernementaux Canada	0	0	4		5	7		16
Tribunal des anciens combattants (révision et appel) Canada	1	0			1	1		3
Total	**722**	**38**	**158**	**23**	**106**	**351**	**29**	**1 427**

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 Canada	58	33	34	158	20	11	314
Gendarmerie royale du Canada	48	26	3	33	4	26	140
Agence du revenu du Canada	10	12	11	12	12	49	106
Défense nationale	14	16	1	25	5	7	68
Agence des services frontaliers du Canada	28	10		18	2	8	66
Citoyenneté et Immigration Canada	6	8	3	14	4	7	42
Emploi et Développement social Canada	5	6	3	3	16	2	35
Société canadienne des postes	4	5		3	12	8	32
Service canadien du renseignement de sécurité	10	9	1	1			21
Affaires autochtones et Développement du Nord Canada	2	6	1	5		5	19
Total	**185**	**131**	**57**	**272**	**75**	**123**	**843**

Les dix institutions visées par le plus grand nombre de plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées en 2014-2015 et au cours de chacun des quatre derniers exercices

Institution	2011-2012	2012-2013	2013-2014	2014-2015
Service correctionnel Canada	326	284	514	314
Gendarmerie royale du Canada	117	182	265	140
Agence du revenu du Canada	65	76	61	106
Défense nationale	115	90	84	68
Agence des services frontaliers du Canada	55	88	56	66
Citoyenneté et Immigration Canada	22	17	53	42
Emploi et Développement social Canada	26	1030	78	35
Société canadienne des postes	22	21	14	32
Service canadien du renseignement de sécurité	32	19	17	21
Affaires autochtones et Développement du Nord Canada	11	18	10	19
Tous les autres ministères et organismes fédéraux	195	448	625	197
Total	**986**	**2 273**	**1 777**	**1 040**

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

Intimé	Règlement rapide	Enquête	Total
Affaires autochtones et Développement du Nord Canada	3	16	19
Affaires étrangères, Commerce et Développement Canada	3	2	5
Agence canadienne d'inspection des aliments	3	2	5
Agence de la santé publique du Canada	1		1
Agence des services frontaliers du Canada	30	36	66
Agence du revenu du Canada	33	73	106
Agriculture et Agroalimentaire Canada	1		1
Anciens Combattants Canada	6	4	10
Bureau du Conseil privé	2	2	4
Bureau du surintendant des institutions financières du Canada	1		1
Centre de la sécurité des télécommunications		1	1
Citoyenneté et Immigration Canada	13	29	42
Commissariat à l'information du Canada		1	1
Commissariat à l'intégrité du secteur public du Canada		2	2
Commissariat au lobbying du Canada	1		1
Commissariat aux langues officielles	1		1
Commission canadienne de sûreté nucléaire		1	1
Commission canadienne des droits de la personne		3	3
Commission de l'immigration et du statut de réfugié du Canada	1	3	4
Commission de la fonction publique du Canada	2		2
Commission des libérations conditionnelles du Canada	2	12	14
Conseil de la radiodiffusion et des télécommunications canadiennes	2		2
Conseil national de recherches Canada		2	2
Défense nationale	20	48	68
École de la fonction publique du Canada	1	1	2
Emploi et Développement social Canada	24	11	35
Énergie atomique du Canada limitée	1		1
Environnement Canada	6	1	7
Financement agricole Canada	2	1	3
Gendarmerie royale du Canada	55	85	140
Industrie Canada	4	7	11

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

Intimé	Règlement rapide	Enquête	Total
Justice Canada	7	7	14
Le service journalistique anglophone de la Société Radio-Canada	4	9	13
Monnaie royale canadienne	1		1
Office des eaux du Nunavut	1		1
Office des transports du Canada		1	1
Patrimoine canadien	1		1
Pêches et Océans Canada	2	12	14
Ressources naturelles Canada	1	2	3
Revera Inc.		1	1
Santé Canada	5	10	15
Secrétariat du Conseil du Trésor du Canada	2	1	3
Service Canada	5	6	11
Service canadien du renseignement de sécurité	11	10	21
Service correctionnel Canada	112	202	314
Service des poursuites pénales du Canada	1		1
Services partagés Canada	3		3
Société canadienne d'hypothèques et de logement	1		1
Société canadienne des postes	16	16	32
Statistique Canada	3	2	5
Transports Canada	4	8	12
Travaux publics et Services gouvernementaux Canada	5	4	9
Tribunal des anciens combattants (révision et appel) Canada	1	1	2
VIA Rail Canada		1	1
Total	**404**	**636**	**1 040**

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

Province ou territoire	Règlement rapide		Enquête		Total (nombre)	Total (pourcentage)
	Nombre	Pourcentage	Nombre	Pourcentage		
Alberta	39	3,75 %	29	2,79 %	68	6,54 %
Colombie-Britannique	55	5,29 %	122	11,73 %	177	17,02 %
Île-du-Prince-Édouard		0,00 %	1	0,10 %	1	0,10 %
Manitoba	13	1,25 %	34	3,27 %	47	4,52 %
Nouveau-Brunswick	9	0,87 %	21	2,02 %	30	2,88 %
Nouvelle-Écosse	12	1,15 %	12	1,15 %	24	2,31 %
Nunavut		0,00 %	2	0,19 %	2	0,19 %
Ontario	141	13,56 %	214	20,58 %	355	34,13 %
Québec	82	7,88 %	158	15,19 %	240	23,08 %
Saskatchewan	22	2,12 %	22	2,12 %	44	4,23 %
Terre-Neuve-et-Labrador	5	0,48 %	3	0,29 %	8	0,77 %
Territoires du Nord-Ouest		0,00 %		0,00 %	0	0,00 %
Yukon	4	0,38 %		0,00 %	4	0,38 %
Autre (sauf les États-Unis)	8	0,77 %		0,00 %	8	0,77 %
États-Unis	1	0,10 %	4	0,38 %	5	0,48 %
Non précisé	2	0,19 %		0,00 %	2	0,19 %
Aucune réponse	11	1,06 %	14	1,35 %	25	2,40 %
Total	**404**	**38,85 %**	**636**	**61,15 %**	**1 040**	**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 à l'issue d'une enquête régulière	Abandonnée	Résolue au moyen du processus de règlement rapide	Réglée	Total
Accès								
Accès	6	35	77	17	65	222	20	442
Correction ou annotation			2		1	2		5
Langue		1				1	1	3
Délais								
Délais	336	2	19		18	70		445
Prorogation	16		12	1	5			34
Correction — Délais						1		1
Protection des renseignements personnels								
Utilisation et communication	711	1	72	5	24	99	7	919
Collecte	4	1	4		12	19	1	41
Conservation et retrait	1		3		3	6		13
Exactitude				1		2		3
Autre					1			1
Total	**1 074**	**40**	**189**	**24**	**129**	**422**	**29**	**1 907**

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 à l'issue d'une enquête régulière	Abandonnée	Résolue au moyen du processus de règlement rapide	Total
Affaires autochtones et Développement du Nord Canada	2		3				6
Affaires étrangères, Commerce et Développement Canada	1						1
Agence des services frontaliers du Canada	13		2				15
Agence du revenu du Canada	8		4			11	23
Anciens Combattants Canada	4					2	6
Bureau du Conseil privé	13		2				15
Citoyenneté et Immigration Canada	14		2		2	3	21
Commission des libérations conditionnelles du Canada			2				2
Défense nationale	24		1		1	4	30
Emploi et Développement social Canada	7		1		1	3	12
Environnement Canada						1	1
Financement agricole Canada						1	1
Gendarmerie royale du Canada	45		2		1	4	52
Industrie Canada	1			1	5	1	8
Justice Canada	1				1		2
Pêches et Océans Canada	8		1		2		11
Santé Canada	5		1			1	7
Service Canada					2	1	3
Service canadien du renseignement de sécurité			1			1	2
Service correctionnel Canada	200	2	7		8	37	254
Société canadienne des postes	1		2				3
Transports Canada	5						5
Total	**352**	**2**	**31**	**1**	**23**	**71**	**480**

Annexe 3 – Processus d'enquête

Accueil :
Des personnes font parvenir des plaintes écrites au Commissariat concernant des infractions à la *Loi sur la protection des renseignements personnels*. L'unité d'accueil examine l'affaire en cause afin de déterminer si elle constitue bel et bien une plainte, c.-à-d. de déterminer si les faits allégués pourraient contrevenir à la *Loi*, ainsi que le moyen le plus efficace de la résoudre. Une personne peut déposer une plainte se rapportant à toute question énoncée à l'article 29 de la *Loi sur la protection des renseignements personnels* — par exemple, le refus d'une institution de communiquer à une personne les renseignements personnels qu'elle détient à son sujet, ou un retard inacceptable dans la communication de ces renseignements; la collecte, l'utilisation ou la communication inappropriée de renseignements personnels; des erreurs dans les renseignements personnels qu'une institution utilise ou communique. L'unité d'accueil réussit parfois à régler immédiatement les problèmes, éliminant ainsi la nécessité pour le Commissariat de s'occuper du dossier comme s'il s'agissait d'une enquête régulière. Dans ces cas-là, nous fermons simplement le dossier, et la plainte est considérée comme ayant été réglée rapidement. La commissaire à la protection de la vie privée peut aussi déposer une plainte si elle est d'avis qu'il y a des motifs suffisants pour mener une enquête.

Plainte?

Non :
La personne est informée, par exemple, que la question ne relève pas de notre organisme.

Oui :
Un enquêteur est affecté au dossier.

Règlement rapide?
Une plainte peut être résolue avant qu'une enquête officielle n'ait commencé si, par exemple, la question a déjà été traitée dans le cadre d'une autre plainte et que l'institution a cessé la pratique, ou si cette pratique ne contrevient pas à la *Loi*.

Enquête régulière :
L'enquête permet d'établir les faits sur lesquels la commissaire s'appuie pour déterminer si les droits des personnes garantis par la *Loi sur la protection des renseignements personnels* ont été enfreints.

L'enquêteur explique à l'institution, par écrit, l'essentiel de la plainte. Il rassemble les faits se rapportant à la plainte en recevant les observations des deux parties, ainsi que par une enquête indépendante, des entrevues avec les témoins et l'examen de la documentation. Au nom de la commissaire à la protection de la vie privée, l'enquêteur a le pouvoir de recevoir des éléments de preuve, d'accéder à des lieux au besoin et d'obtenir ou d'examiner des copies de dossiers trouvés sur place.

Abandonnée?
Une plainte peut être abandonnée si, par exemple, un plaignant décide de ne pas continuer avec sa plainte, ou s'il ne peut être localisé.

Analyse (suite)

Résolue? (suite)

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

Analyse :

L'enquêteur analyse les faits et prépare les recommandations pour la commissaire à la protection de la vie privée ou son délégué. L'enquêteur communique avec les parties et examine les faits recueillis au cours de l'enquête. Il informe également les parties des recommandations, fondées sur les faits, qu'il présentera à la commissaire à la protection de la vie privée ou à son délégué. À cette étape, les parties peuvent formuler d'autres observations.

Au besoin, des consultations internes sont effectuées avec, par exemple, le concours de la Division des services juridiques ou de la Direction de la recherche et des politiques.

Résolue?

Le CPVP cherche à régler les plaintes et à prévenir d'autres infractions à la *Loi*. La commissaire favorise la résolution des différends par l'entremise de la médiation, de la négociation et de discussions persuasives. L'enquêteur participe au processus.

Conclusion :

La commissaire à la protection de la vie privée ou son délégué examine le dossier, évalue le rapport et prend une décision au sujet de la recommandation. La commissaire ou son délégué, et non l'enquêteur, décide de l'issue appropriée du dossier et s'il faut présenter des recommandations à l'institution.

La commissaire à la protection de la vie privée ou son délégué envoie une lettre expliquant ses conclusions aux parties. Cette lettre présente le fondement de la plainte, les faits établis, l'analyse effectuée par la commissaire ou son délégué, ainsi que toute recommandation faite à l'institution. La commissaire à la protection de la vie privée ou son délégué peut demander à l'institution de lui indiquer par écrit, dans un délai précis, les mesures prévues pour mettre en œuvre les recommandations.

Les conclusions possibles sont les suivantes :

Non fondée : La preuve ne permet pas à la commissaire à la protection de la vie privée ou à son délégué de conclure que les droits du plaignant en vertu de la *Loi* ont été enfreints.

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

Fondée et résolue : L'enquête permet de justifier les allégations, et l'institution s'engage à prendre des mesures correctives pour remédier au problème.

Résolue : La preuve recueillie au cours de l'enquête soutient les allégations soulevées dans la plainte, mais l'institution s'engage à prendre des mesures pour corriger le problème; à la satisfaction du Commissariat. Cette conclusion est tirée dans les situations où, compte tenu que la plainte découle principalement d'un problème de communication, il serait trop sévère de conclure qu'elle est fondée.

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

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

Lorsqu'on lui refuse l'accès à ses renseignements personnels, le plaignant, ou la commissaire à la protection de la vie privée, peut choisir de demander une audience à la Cour fédérale. La Cour fédérale a le pouvoir d'examiner l'affaire et de déterminer si l'institution doit fournir les renseignements au requérant.

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

Annexe 4 – Rapport 2014–2015 du commissaire spécial à la protection de la vie privée

Pour la période du rapport 2014–2015, deux personnes ont occupé le poste de commissaire spécial à la protection de la vie privée et ont présenté les rapports qui suivent.

JOHN H. SIMS, C.R., POUR LA PÉRIODE DU 1ER AVRIL AU 15 DÉCEMBRE 2014

Pour une deuxième année, j'ai le plaisir de rendre compte des activités du bureau du commissaire spécial à la protection de la vie privée. Depuis le 1er avril 2007, le Commissariat à la protection de la vie privée (CPVP) est assujetti à la *Loi sur la protection des renseignements personnels*. La loi qui a entraîné ce changement n'a pas créé simultanément de mécanisme distinct pour enquêter sur les plaintes relatives à des demandes de communication qui n'auraient pas été traitées comme il se doit par le CPVP.

Compte tenu d'un principe essentiel du droit de l'accès à l'information qui veut que les décisions sur la communication des renseignements gouvernementaux fassent l'objet d'un examen indépendant, on a créé le poste de commissaire spécial à la protection de la vie privée qui a le pouvoir d'enquêter sur les plaintes concernant le CPVP.

Plus précisément, conformément au paragraphe 59(1) de la *Loi sur la protection des renseignements personnels*, la commissaire à la protection de la vie privée m'a délégué, à titre de commissaire spécial à la protection de la vie privée,

> *Les pouvoirs et les fonctions du commissaire à la protection de la vie privée énoncés dans les articles 29 à 35 et 42 de la* Loi, *sous réserve des restrictions et limites suivantes :*
>
> *Conformément à l'alinéa 59(2)*a*), le délégataire ne fera pas enquête à l'égard de toute plainte découlant d'un refus de communiquer des renseignements personnels en vertu de l'alinéa 19(1)*a*) ou* b*) ou de l'article 21 de la* Loi.

J'étais la quatrième personne à occuper ce poste.

Deux plaintes de l'an dernier étaient toujours à l'étude au début de l'exercice, et trois nouvelles ont été déposées. Trois des cinq plaintes ont été réglées, dont **aucune n'était fondée**. L'enquête sur les deux dernières plaintes (toutes deux liées au même incident) n'était pas terminée à la fin de l'exercice. Les conclusions de cette enquête feront partie du prochain rapport annuel.

La principale question au cœur des trois plaintes réglées était l'application appropriée de l'article 22.1 de la *Loi sur la protection des renseignements personnels*. Dans le premier cas, l'exception obligatoire empêche la communication de renseignements personnels obtenus ou créés par le CPVP pendant une enquête. Toutefois, une fois l'enquête et toutes les procédures connexes terminées, l'exception est partiellement annulée. C'est alors que le paragraphe 22.1(2) de la *Loi* prévoit que le CPVP ne doit pas refuser de communiquer des renseignements personnels créés par le commissaire ou en son nom.

Dans chacune des trois plaintes résolues, une personne a demandé des documents relatifs à une enquête menée par le CPVP. Dans un cas, les enquêtes du CPVP étaient terminées au moment de la présentation des demandes d'information. Dans un autre cas, l'enquête était toujours en cours au moment du dépôt de la demande d'information.

Selon notre examen des plaintes, chaque fois, le CPVP a appliqué l'exception correctement. Dans le cas des enquêtes terminées, il l'a appliquée seulement à l'égard des renseignements personnels qu'il a obtenus lors de ces enquêtes.

En ce qui concerne l'enquête en cours, le CPVP a appliqué l'exception à tous les documents liés à ce dossier, qu'il les ait obtenus ou créés pendant l'enquête.

Les trois plaintes ont également soulevé des questions secondaires. Dans certains cas, par exemple, le CPVP a appliqué l'exception correctement pour empêcher la communication de certains documents étant donné qu'ils ne contenaient pas de renseignements personnels relatifs au demandeur, mais plutôt à un autre individu (article 26), ou qu'ils ne contenaient pas du tout de renseignements personnels (article 12).

Enfin, l'une des trois plaintes résolues a aussi soulevé des préoccupations au sujet de la façon dont deux autres ministères gouvernementaux ont traité les renseignements personnels du demandeur, ainsi que de la façon dont le CPVP a enquêté sur les plaintes concernant ces ministères. Le bureau du commissaire spécial à la protection de la vie privée n'a cependant pas le pouvoir de régler ces questions. Il a pour mandat de recevoir les plaintes liées au traitement inapproprié par le CPVP de renseignements personnels qu'il détient et de mener des enquêtes sur ce type de plainte. Il ne peut pas examiner comment le CPVP mène ses enquêtes ou comment d'autres ministères gèrent les renseignements personnels.

Les quatrième et cinquième plaintes portent toutes deux sur la perte d'un disque dur amovible contenant des renseignements personnels de nature sensible liés au personnel du Commissariat à la protection de la vie privée et du Commissariat à l'information. L'enquête n'était pas terminée à la fin de l'exercice même si, à la date de rédaction du présent rapport, elle l'était en bonne partie. Les conclusions figureront dans le prochain rapport annuel.

Ce fut un privilège pour moi de remplir un mandat à titre de commissaire spécial à la protection de la vie privée. L'existence de ce poste assure l'intégrité du processus de traitement des plaintes, un élément essentiel de tout régime d'accès à l'information. Je suis honoré d'y avoir participé.

Le tout respectueusement soumis,

John H. Sims, c.r.

DAVID LOUKIDELIS, C.R., DU 16 DÉCEMBRE 2014 AU 31 MARS 2015

Le poste de commissaire spécial à la protection de la vie privée a été créé à la suite de l'assujettissement, en 2007, du Commissariat à la protection de la vie privée (CPVP) à la *Loi sur la protection des renseignements personnels*. La loi qui a amené ce changement n'a pas créé un processus distinct d'enquête sur les plaintes relatives aux réponses du CPVP aux demandes de communication présentées à une institution en vertu de la *Loi*.

Compte tenu d'un principe essentiel du droit de l'accès à l'information qui veut que les décisions sur la communication des renseignements gouvernementaux fassent l'objet d'un examen indépendant, on a créé le poste de commissaire spécial à la protection de la vie privée qui a le pouvoir d'enquêter sur les plaintes relatives au CPVP. Le rôle de mon bureau est d'enquêter sur les plaintes selon lesquelles le CPVP n'a pas répondu de manière appropriée aux demandes d'accès qui lui ont été soumises à titre d'institution.

Je suis la cinquième personne à occuper ce poste depuis 2007. Comme j'ai été nommé en décembre 2014, j'ai le plaisir de rendre compte pour la première fois des activités de mon bureau.

Plaintes actives de l'exercice précédent

Deux plaintes de l'année dernière étaient toujours à l'étude en début d'exercice. Elles ont trait à l'enquête en cours sur le disque dur qu'a perdu le CPVP en 2014. Mon prédécesseur, John Sims, examine actuellement la question et pourra clore les dossiers de ces plaintes dès qu'il aura terminé son enquête.

Nouvelles plaintes déposées au cours du présent exercice

Au début de mon mandat, j'ai reçu trois plaintes, dont deux provenaient de la même personne.

Un plaignant a demandé la tenue d'une enquête sur le support utilisé pour la réponse fournie à sa demande d'accès au CPVP, ainsi que sur les exceptions appliquées en vertu des articles 22.1 et 26 de la *Loi sur la protection des renseignements personnels*. Il a aussi allégué que ses renseignements personnels avaient été interceptés et surveillés par un gouvernement étranger.

Mon enquête s'est limitée à la plainte concernant les exceptions appliquées, le support utilisé pour la réponse à la demande et le processus de recherche. Les allégations selon lesquelles ses renseignements personnels ont été interceptés et surveillés par des organismes gouvernementaux étrangers ne relèvent pas de mon mandat.

En raison de la préoccupation du plaignant au sujet du support utilisé par le CPVP pour répondre à sa demande, j'ai vérifié si le CPVP avait respecté l'article 17.1 de la *Loi sur la protection des*

renseignements personnels. Le plaignant souhaitait obtenir des copies papier des documents pertinents, et non des copies électroniques, comme celles que lui avait fournies le CPVP.

L'article 17.1 ne précise pas si on doit communiquer les renseignements personnels demandés sur support électronique ou papier. Il y est seulement question de « délivrance de copies ». À l'ère informatique, on fournit la plupart des documents pertinents liés à une demande sous forme électronique et, lorsqu'on remet des copies papier, elles sont numérisées à l'aide d'un logiciel utilisé pour le traitement des demandes de communication. Afin de tenir compte de l'environnement et de réduire les coûts, la plupart des institutions du gouvernement du Canada communiquent les documents sur un CDROM lorsque le volume de documents est important. Le CPVP a comme politique de fournir un CDROM si la demande totalise plus de 100 pages, ce qui était le cas en l'espèce. Il a cependant indiqué qu'il aurait fourni les documents sur le support demandé si le plaignant le lui avait demandé.

La plainte de l'individu au sujet des exceptions avait trait à la pertinence de leur application en vertu du paragraphe 22.1(1) et de l'article 26 de la *Loi sur la protection des renseignements personnels*. Selon le paragraphe 22.1(1), le CPVP n'est pas tenu de communiquer à un demandeur des renseignements qu'il a « obtenus » ou « créés » dans le cadre d'une enquête. Il s'agit d'une exception obligatoire : si celleci s'applique, le CPVP est obligé de refuser la communication. Toutefois, une fois l'enquête et toutes les procédures connexes terminées, l'exception est annulée en partie. Elle ne s'applique alors plus aux documents créés pendant l'enquête. Mon enquête a révélé que les documents contestés avaient été obtenus pendant le cours des propres enquêtes du CPVP. Ce dernier a, par conséquent, appliqué correctement l'exception obligatoire visée par le paragraphe 22.1(1) en refusant de communiquer les documents.

L'article 26 de la *Loi sur la protection des renseignements personnels* établit que la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui portent sur un autre individu que celui qui fait la demande doit être refusée si elle est interdite aux termes de l'article 8. L'examen des documents auxquels s'est appliqué l'article 26 dans le présent cas a permis de confirmer que les renseignements exemptés n'étaient pas les renseignements personnels du plaignant. L'article 26 a été appliqué afin de protéger les noms des individus qui ne sont pas des employés du gouvernement du Canada. J'en ai conclu que cela était conforme à l'article 26.

Les deux autres plaintes dont il est question ici ont été déposées par la même personne et sont liées à la même demande présentée au CPVP. Le plaignant allègue que le CPVP avait indûment refusé de lui communiquer des renseignements personnels en vertu du paragraphe 22.1(1). Il a aussi soutenu que le CPVP n'avait pas demandé comme il se doit une prorogation du délai et qu'il avait également répondu en retard.

Comme dans le cas de la première plainte susmentionnée, mon enquête a révélé que les documents contestés avaient été obtenus pendant les propres enquêtes du CPVP. J'ai donc conclu que le CPVP avait appliqué correctement le paragraphe 22.1(1) en refusant de communiquer ces documents.

En ce qui concerne la prorogation du délai et le temps de réponse, l'enquête a révélé que la demande totalisait 8 850 pages pertinentes. La division de l'accès à l'information et de la protection de la vie privée du CPVP est composée d'un directeur et de deux analystes principaux. Au cours de l'exercice financier 20132014, elle a reçu 130 demandes de communication, 25 consultations sur l'accès à l'information, 32 demandes de communication de renseignements personnels et 7 consultations sur la protection des renseignements personnels. Selon le CPVP, le respect du délai de 30 jours aurait entravé de façon sérieuse son fonctionnement, car il aurait été dans l'impossibilité de s'acquitter de ses obligations législatives relatives aux autres demandes alors en cours de traitement.

Il va sans dire qu'il aurait été pour le moins difficile pour l'un des analystes principaux (ou même pour les deux) d'examiner 8 850 pages de documents et de décider des parties pouvant être communiquées dans le délai de 30 jours. De plus, la division de l'accès à l'information et de la protection de la vie privée du CPVP allait avoir, dans le cours normal des choses, d'autres demandes à traiter au même moment, sans oublier les tâches courantes à accomplir. Tenter de répondre à la demande du plaignant qui visait un aussi grand volume de documents aurait eu, on s'en doute, un effet négatif sur la capacité de la division d'exécuter ses autres tâches. Essayer de « tout mettre de côté » pour répondre à la demande dans le délai de 30 jours aurait compromis les droits des autres personnes.

Finalement, j'ai conclu que l'observation du délai de 30 jours aurait entravé de façon sérieuse le fonctionnement du CPVP et que ce dernier pouvait, par conséquent, proroger de 30 jours le délai de réponse en vertu de l'article 15.

Quant à la plainte concernant le retard de la réponse, compte tenu de la prorogation de 30 jours du délai, le CPVP devait fournir une réponse dans les 60 jours civils. Le temps nécessaire pour que le demandeur reçoive la réponse par courrier ou par tout autre mode de livraison n'est pas calculé dans le temps alloué. Dans le présent cas, le CPVP a utilisé le service Colis accélérés de Postes Canada pour envoyer sa réponse au plaignant. Le délai du service peut varier selon la destination et d'autres facteurs, et le temps qu'il faut compter pour qu'une lettre ou un colis arrive à destination n'est pas du ressort de l'expéditeur. En dernière analyse, j'ai conclu que cet aspect de la plainte était lui aussi non fondé.

David Loukidelis, c.r.