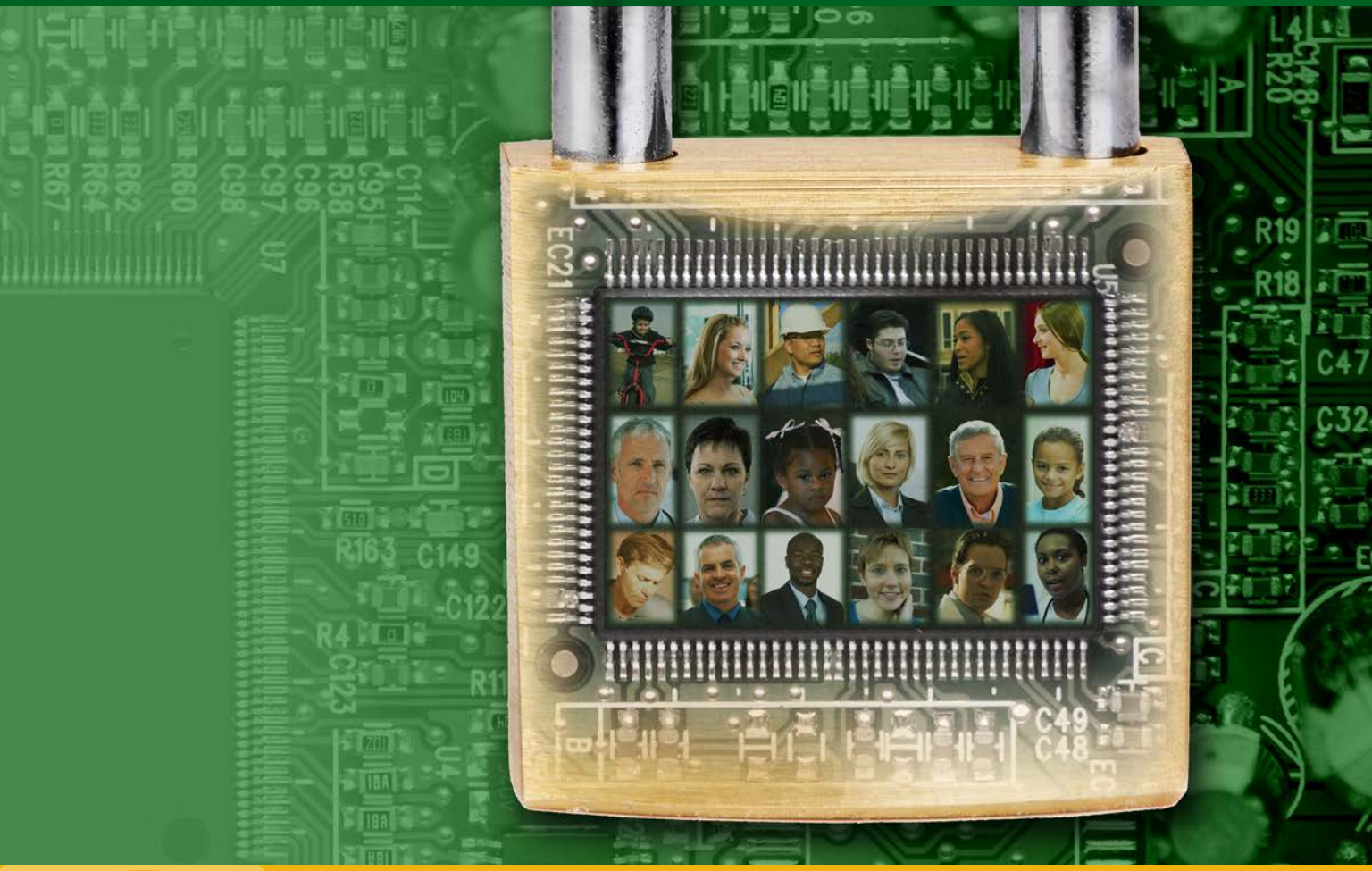
Commissariat
à la protection de
la vie privée du Canada

Sécuriser le droit à la vie privée



Rapport annuel au Parlement 2012-2013

Rapport concernant la
Loi sur la protection des renseignements personnels

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario) K1A 1H3

613-947-1698, 1-800-282-1376
Télécopieur : 613-947-6850
ATS : 613-992-9190

N° de cat. IP50-2013F-PDF
1913-7559

Cette publication se trouve également sur notre site Web à **www.priv.gc.ca**

Suivez-nous sur Twitter : @PrivacyPrivee

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Octobre 2013

L'honorable Noël A. Kinsella, 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 2012 au 31 mars 2013, conformément à l'article 38 de la *Loi*.

Veuillez agréer, Monsieur le Président, l'assurance de ma considération distinguée.

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

original signé par

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Octobre 2013

L'honorable Andrew Scheer, député
Président
La Chambre des communes
Ottawa (Ontario) K1A 0A6

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels* pour la période du 1er avril 2012 au 31 mars 2013, conformément à l'article 38 de la *Loi*.

Veuillez agréer, Monsieur le Président, l'assurance de ma considération distinguée.

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

original signé par

Jennifer Stoddart

Table des matières

1.0 Message de la commissaire

Pour sécuriser le droit à la vie privée : énoncer le devoir de diligence du gouvernement

En présentant mon dernier rapport annuel à titre de commissaire à la protection de la vie privée, qui met l'accent sur assurer le droit à la vie privée, je tiens à souligner l'importance vitale de la responsabilité du gouvernement de recueillir uniquement les renseignements dont il a besoin pour gouverner, comme cela est justifié dans une société libre et démocratique, et de traiter les renseignements personnels de la population canadienne avec le plus grand respect.

Il ne s'agit pas uniquement d'un rôle de dépositaire. On parle ici de la relation entre les citoyens et l'État, dans le cadre de laquelle des restrictions aux libertés fondamentales ne peuvent être imposées que si le gouvernement réussit à en démontrer la nécessité et seulement d'une façon qui honore la confiance que lui portent les citoyens.

Les Canadiennes et les Canadiens fournissent leurs renseignements personnels au gouvernement par obligation, souvent sous contrainte légale. De fait, la prestation efficace d'importants services gouvernementaux l'exige. En retour, les gens s'attendent à juste titre à ce que le gouvernement gère ces renseignements de façon responsable et efficace.

Le public de plus en plus inquiet

Il est clair, cependant, que nombre de Canadiennes et de Canadiens se demandent s'il en est ainsi. En fait, dans un sondage téléphonique national réalisé pour le Commissariat en 2012-2013, seulement 21 % des répondants étaient d'avis que les gouvernements prenaient au sérieux leur responsabilité de protéger les renseignements personnels. Bien que les réponses données à la même question au sujet des entreprises du secteur privé dénotent encore plus de scepticisme de la part des répondants (seulement 13 % d'entre eux estimaient que les entreprises prenaient au sérieux leur responsabilité), cela n'en demeure pas moins décourageant.

De façon plus générale, le sondage a aussi révélé que les deux tiers des Canadiens se disent préoccupés par la protection de leurs renseignements personnels. Le quart d'entre eux se disent même « extrêmement » préoccupés par cette question. Ils se posent des questions sur leur propre capacité à protéger leurs renseignements personnels — 56 % des répondants ne croient pas avoir une bonne compréhension du risque que représentent les nouvelles technologies pour leur vie privée. Or, nous avons constaté que ce manque de confiance augmente de manière constante depuis l'an 2000.

Le malaise croissant des Canadiens au sujet de la protection de leur vie privée n'est pas surprenant. De nouvelles technologies apparaissent et se répandent rapidement, bon nombre d'entre elles étant alimentées par des utilisations novatrices et considérables des renseignements personnels qu'il peut être difficile, voire impossible, de comprendre dans leur totalité. Les gens sont aussi inondés de demandes exigeant de plus en plus de renseignements personnels; par ailleurs, ils entendent souvent parler d'atteintes à la sécurité des renseignements personnels et de fuites de renseignements personnels d'une grande ampleur.

Des exemples qui minent la confiance

Le présent rapport annuel présente, malheureusement, de nombreux exemples associés au secteur public qui illustrent les types d'enjeux qui avivent les inquiétudes générales des Canadiennes et des Canadiens à l'égard de la protection de la vie privée, tout en sapant leur confiance envers les ministères et les organismes fédéraux qui recueillent leurs renseignements personnels.

Par exemple, une vérification de l'Agence du revenu du Canada (ARC), qui traite quotidiennement des renseignements financiers de nature délicate concernant des Canadiennes et des Canadiens, a permis de constater que des employés avaient eu accès aux dossiers de contribuables sans autorisation, et ce, à maintes reprises. Bon nombre de ces atteintes sont passées inaperçues pendant plusieurs années.

Des éléments d'information indiquent également un accroissement du temps de réponse aux demandes de renseignements personnels présentées en vertu de la *Loi sur la protection des renseignements personnels*, ainsi qu'aux demandes du Commissariat dans le cadre d'enquêtes et d'autres affaires.

Pour la troisième année consécutive, le nombre d'atteintes à la sécurité des données signalées au Commissariat n'a jamais été aussi élevé. Parmi les incidents décrits dans le présent rapport, mentionnons la perte d'un disque dur contenant les renseignements personnels de plus de 500 000 bénéficiaires de prêts étudiants.

L'augmentation du nombre d'atteintes à la sécurité des renseignements personnels signalées laisse peut-être entrevoir une perte de données plus importante de la part des institutions, mais il se pourrait aussi qu'elle indique simplement que les ministères font preuve d'une diligence accrue pour respecter leurs obligations en matière de signalement des atteintes. Or, même si cette dernière hypothèse était la bonne et dans le meilleur des scénarios, la

population canadienne serait en droit d'exiger qu'on accorde plus d'attention aux pratiques de traitement de l'information afin d'éviter les atteintes au départ.

Parmi les autres exemples d'intérêt figurant dans le présent rapport, mentionnons la collecte non justifiée de renseignements personnels par deux ministères fédéraux à partir de la page Facebook personnelle d'une militante pour les droits des Premières Nations; l'utilisation abusive du dossier médical confidentiel d'un membre des Forces canadiennes par un ex-conjoint, et l'utilisation d'une base de données d'application de la loi par un employé de la Gendarmerie royale du Canada afin de vérifier les antécédents d'une personne à qui il envisageait de louer un appartement.

Une décennie marquée par le changement

Le Commissariat a fait état d'atteintes semblables au cours de la dernière décennie, soit depuis que j'occupe le poste de commissaire, mais l'utilisation sans cesse croissante de la technologie a une incidence considérable sur les problèmes observés. Les efforts déployés par le gouvernement fédéral afin de moderniser ses services ainsi que ses procédés et outils de travail s'accompagneront inévitablement d'une augmentation du nombre de renseignements personnels recueillis, conservés et communiqués à l'aide d'appareils et de plate-formes électroniques.

L'innovation est essentielle et elle peut offrir de nombreux avantages, mais elle peut aussi introduire des vulnérabilités dans les processus. Le gouvernement doit veiller à ce que les politiques et les procédures en matière de protection de la vie privée évoluent en conséquence. Nous ne devrions jamais oublier les valeurs humaines et les décisions individuelles que la technologie cherche à appuyer. La protection de la vie privée s'inscrit dans un souci d'autonomie, de dignité et d'intégrité à l'égard des citoyens que servent les gouvernements; il ne s'agit pas d'une fin en soi.

Les progrès technologiques considérables réalisés au cours de la dernière décennie ont été accompagnés d'une volonté, à l'échelle internationale, de renforcer la sécurité nationale et publique. Depuis mon entrée en poste, le Commissariat s'efforce de faire valoir que ni la sécurité ni la protection de la vie privée ne constitue un droit absolu, et qu'aucune des deux ne devrait être mis de côté ou abandonné au profit de l'autre.

En 2011, les gouvernements canadien et américain ont convenu de mettre en place une série d'initiatives visant à faciliter le commerce et à accroître la sécurité. Un grand nombre de ces initiatives prévoient l'échange d'une plus grande quantité de renseignements sur les déplacements des personnes entre les deux pays. Compte tenu des répercussions sur la protection de la vie privée que ces initiatives sont susceptibles d'entraîner, le Commissariat s'est engagé à surveiller de près leur évolution. Vous trouverez, dans le présent rapport, le fruit de quelques-unes de nos réflexions sur des enjeux clés.

La reddition de comptes est vitale

Bien que le présent rapport mette en lumière les menaces à la protection des renseignements personnels ainsi que les risques d'atteinte à la vie privée que présentent certaines initiatives gouvernementales mises en place pour renforcer la sécurité publique, il existe de nombreux autres exemples de situations où le gouvernement n'a pas traité les renseignements personnels qu'il détient de la façon dont la population canadienne est en droit de s'attendre à ce qu'il le fasse.

Les ministères et les organismes ont un accès inégalé aux renseignements les plus personnels des individus, ce qui rend l'obligation de rendre des comptes d'autant plus vitale. S'ils ne voient pas les institutions fédérales mettre en place des mesures pour s'acquitter de leurs obligations en matière de protection des renseignements personnels, les Canadiennes et les Canadiens se demanderont si leurs renseignements personnels sont en sécurité. De la même façon, si les institutions continuent de faire traîner en longueur le processus donnant accès aux citoyens à leurs renseignements personnels ou la collaboration avec le Commissariat en réponse aux plaintes, des questions fondamentales seront soulevées quant à l'efficacité du régime canadien de protection de la vie privée.

Le fait que le gouvernement n'a toujours pas apporté de modifications à la *Loi sur la protection des renseignements personnels* en vue de la moderniser est également préoccupant. La *Loi* a permis d'établir des règles de base relativement à la façon dont les ministères et les organismes gouvernementaux traitent les renseignements personnels et elle continue d'être utile à cette fin, cela dit, le monde a énormément changé depuis son adoption il y a plus de trente ans. Les préoccupations et les attentes de la population canadienne ont évolué parallèlement aux progrès technologiques, et des pressions salutaires se sont mises à peser sur le gouvernement et les citoyens. Afin de préserver sa légitimité et sa crédibilité, ainsi que de conserver la confiance des citoyens, le gouvernement doit également apporter des modifications à ses mécanismes d'intendance des renseignements personnels, et je crois fermement que la mise à jour de la *Loi sur la protection des renseignements personnels* permettra non seulement de moderniser la *Loi*, mais aussi d'indiquer clairement aux fonctionnaires et aux citoyens que le gouvernement fédéral prend au sérieux sa responsabilité de protéger les renseignements personnels.

Un départ dans la confiance

Compte tenu de l'échéance prochaine de mon mandat, je n'aurai pas la chance d'assister à la modernisation de la *Loi sur la protection des renseignements personnels* à titre de commissaire. Je suis toutefois très fière de savoir que le travail accompli par le Commissariat a mené à l'apport d'améliorations notables dans l'ensemble du gouvernement fédéral au chapitre de la protection du droit à la vie privée. Bien que le présent rapport souligne de nombreuses lacunes en ce qui a trait aux pratiques de traitement de l'information des institutions fédérales, je tiens à souligner que j'ai également été témoin de la mise en œuvre

de nombreux programmes de qualité ainsi que d'améliorations encourageantes à l'égard de la protection de la vie privée au cours de mon mandat. De plus, j'ai rencontré d'innombrables fonctionnaires déterminés à veiller au respect du droit à la vie privée de la population canadienne.

Maintenant que je m'apprête à relever de nouveaux défis, je tiens à remercier en particulier le personnel exceptionnellement dévoué et professionnel du Commissariat, qui m'a soutenue tout au long de mon mandat. Je me sens très privilégiée et honorée d'avoir travaillé avec un groupe de personnes aussi engagées, et je suis convaincue qu'il continuera à défendre le droit de la population canadienne à la vie privée et le caractère d'inviolabilité des renseignements personnels pendant la période de transition du Commissariat vers une nouvelle direction.

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

1.1 BILAN DE L'ANNÉE

Principales réalisations en 2012-2013

La présente section présente un bref aperçu du travail accompli par le Commissariat au cours du dernier exercice pour protéger et renforcer le droit à la vie privée de la population canadienne dans ses échanges avec le gouvernement du Canada.

Vérifications de la conformité à la *Loi sur la protection des renseignements personnels*

Nous avons procédé à une vérification de l'Agence du revenu du Canada (ARC) et du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).

La vérification de l'ARC, qui est décrite en détail au chapitre 3, faisait suite à de multiples incidents flagrants d'atteinte à la vie privée survenus à l'Agence, dont certains concernaient plusieurs communications de dossiers de contribuables passées inaperçues pendant des années.

Nous avons constaté que, même si l'ARC s'est dotée de politiques et de pratiques solides en matière de protection de la vie privée, il existe des faiblesses graves sur le plan de la mise en place et de la surveillance de celles-ci.

En tout, nous avons formulé, à l'intention de l'ARC, 14 recommandations concernant les points suivants : la gestion des cas d'atteinte à la vie privée; l'accès aux renseignements par les employés et la surveillance

de ces derniers; la sécurité des technologies de l'information; la gestion de la protection de la vie privée et la responsabilité à cet égard. L'Agence a accepté toutes nos recommandations et y a répondu par un plan d'action concret et un calendrier de mise en œuvre des améliorations. Dans deux ans, nous vérifierons si l'ARC a bien mis en place tous les changements promis.

Au chapitre 5, nous décrivons notre vérification de CANAFE, qui doit avoir lieu tous les deux ans en vertu d'une disposition de la loi régissant l'institution.

Nous avons constaté que CANAFE a réalisé peu de progrès dans la mise en œuvre de cinq des dix recommandations formulées lors de notre vérification précédente, qui a été réalisée en 2009. Nous lui avons encore une fois recommandé de régler ces questions récurrentes.

CANAFE continue de recevoir et de conserver des renseignements personnels qui n'ont pas de lien direct avec ses programmes ou activités, et dont il n'a pas besoin ou dont il ne se sert pas. Tant que cette situation perdurera, il y aura un écart entre les pratiques de CANAFE et ses obligations en vertu de la *Loi sur la protection des renseignements personnels*.

Demandes de renseignements et plaintes

Le Centre d'information, qui est l'un des éléments de la ligne de front du Commissariat à la protection de la vie privée du Canada, répond aux demandes de renseignements présentées par des particuliers et des organisations au sujet du droit à la vie privée et des responsabilités à cet égard. En 2012-2013, nous avons reçu près de 10 000 demandes de renseignements, dont plus du quart concernait le secteur public fédéral.

C'est presque deux fois le nombre de demandes de renseignements reçues au cours de l'exercice précédent à l'égard d'inquiétudes concernant la protection de la vie privée dans le secteur fédéral, ce qui montre l'importance de ce service auprès de la population canadienne. Ce nombre sans précédent de demandes est en partie attribuable aux nombreuses préoccupations exprimées au sujet de graves cas d'atteinte à la sécurité des renseignements personnels survenus au cours de la dernière année.

Nous avons aussi constaté un accroissement des cas de plaintes multiples présentées par un même plaignant — au cours du dernier exercice, 251 plaintes ont été déposées par 18 personnes ayant présenté chacune huit plaintes ou plus. En outre, le nombre de plaintes relatives au dépassement, par les institutions, du délai prescrit par la loi pour répondre aux demandes de communication individuelles a atteint un sommet inégalé.

En revanche, la proportion de plaintes réglées avec succès par la négociation ou la médiation a augmenté. Cette approche de règlement rapide a permis de clore le tiers des dossiers au cours du dernier exercice, par rapport au quart l'année précédente.

Atteintes à la sécurité des renseignements personnels

Un autre record a été établi en 2012-2013 pour ce qui est du nombre d'atteintes à la sécurité des renseignements personnels déclarées au Commissariat par les institutions fédérales, soit 109. Il s'agit d'une augmentation de plus du tiers comparativement à l'année précédente. Comme toujours, du fait que les ministères et les organismes ne sont pas obligés de nous informer des atteintes, il nous est impossible de savoir si la hausse est attribuable à une augmentation réelle du nombre d'atteintes ou à une plus grande diligence en matière de signalement des cas.

Évaluations des facteurs relatifs à la vie privée (EFVP)

Les institutions fédérales sont tenues d'évaluer les facteurs relatifs à la vie privée des activités et des initiatives qui nécessitent l'utilisation de renseignements personnels. En réalisant une EFVP, une organisation peut cerner les risques éventuels d'atteinte à la vie privée liés à une activité prévue et expliquer comment elle les atténuera.

Nous avons reçu 68 nouvelles EFVP en 2012-2013, et bon nombre d'entre elles avaient trait à des programmes actuellement mis en œuvre dans le cadre du plan d'action canado-américain *Par-delà la frontière* (voir le chapitre 5).

Nous avons conclu que 21 de ces EFVP faisaient état de risques particuliers d'atteinte à la vie privée, ce qui nous a amenés à formuler des recommandations détaillées et exhaustives en vue de l'apport d'améliorations. Certaines de ces recommandations sont présentées au chapitre 6.

Politiques et affaires parlementaires

En 2012-2013, le Commissariat a comparu neuf fois devant des comités parlementaires et soumis deux mémoires écrits. Nous avons réalisé des analyses en profondeur de huit projets de loi et de trois études réalisées par des comités parlementaires sur des sujets liés à la protection de la vie privée, comme l'utilisation croissante des médias sociaux. Le Commissariat a aussi continué à surveiller plusieurs autres mesures législatives susceptibles d'avoir des répercussions sur la protection des renseignements personnels.

Le projet de loi omnibus du gouvernement (projet de loi C-45) a soulevé plusieurs enjeux possibles en matière de vie privée parce qu'il prévoyait l'accroissement des mesures de sécurité frontalières touchant les voyageurs à destination et en provenance du Canada. Le projet de loi C-55 est une autre mesure législative importante examinée par le Parlement; il clarifiait les circonstances et les mécanismes juridiques mis en place concernant l'utilisation d'interceptions de communications électroniques faites sans mandat par des services policiers en situation d'urgence.

Nous avons aussi présenté des observations sur les incidences possibles sur la protection de la vie privée de deux projets de loi sur la transparence financière — le projet de loi C-27, qui vise les Premières

Nations, et le projet de loi C-377, qui vise les syndicats.

Sensibilisation auprès des institutions fédérales

La sensibilisation auprès des institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels* est une partie essentielle de notre travail dans le secteur public. Parmi les activités de sensibilisation menées au cours de l'exercice, mentionnons le quatrième atelier annuel sur l'évaluation des facteurs relatifs à la vie privée à l'intention des fonctionnaires, qui mettait l'accent sur les technologies de l'information, la protection des renseignements personnels et la sécurité, ainsi que sur les EFVP touchant des institutions multiples. Nous avons aussi profité de l'activité pour lancer une nouvelle vidéo sur les EFVP, conçue pour aider les ministères et les organismes fédéraux à respecter les exigences de la Directive du Secrétariat du Conseil du Trésor sur l'évaluation des facteurs relatifs à la vie privée, tout en soulignant les attentes du Commissariat.

Dans le cadre d'une autre activité, le Commissariat a discuté de ses initiatives visant à moderniser ses processus d'enquête avec les agents responsables des unités de l'accès à l'information et de la protection des renseignements personnels (AIPRP) de 12 institutions fédérales faisant habituellement l'objet d'un nombre de plaintes relatives à la protection de la vie privée plus élevé que la moyenne.

Pour souligner la Journée de la protection des données (le 28 janvier 2013), le Commissariat a produit des affiches mettant en vedette ses populaires illustrations sur la protection de la vie privée et les a distribuées aux coordonnateurs de l'AIPRP et à d'autres professionnels de la protection de la vie privée et de la sécurité au sein du gouvernement fédéral.

Avancement du savoir

Compte tenu de l'évolution rapide du contexte dans lequel s'inscrit la protection de la vie privée, en partie en raison du rythme effréné des changements technologiques, il est essentiel que les spécialistes du Commissariat se tiennent à la fine pointe en matière de recherche.

Au cours du dernier exercice, par exemple, nous avons élaboré des rapports de recherche sur la technologie de reconnaissance faciale, l'analyse prédictive, ce qu'une adresse Internet peut révéler sur un utilisateur, ainsi que les incidences sur la protection de la vie privée des véhicules aériens sans pilote.

De plus, le Commissariat a travaillé avec certains de ses homologues provinciaux à l'élaboration d'une trousse d'urgence pour la protection des renseignements personnels dans le but de faciliter les communications en situation d'urgence, tout en respectant la nécessité de protéger les renseignements personnels.

1.2 LA PROTECTION DE LA VIE PRIVÉE EN CHIFFRES EN 2012-2013

Demandes de renseignements

Liées à la *Loi sur la protection des renseignements personnels*	**2 599**
Liées à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)	4 349
Demandes n'étant pas exclusivement liées à l'une ou l'autre des lois	2 940
Total	**9 888**

Plaintes liées à la *Loi sur la protection des renseignements personnels

Plaintes liées à la *Loi sur la protection des renseignements personnels* en 2012 2013	
Catégorie	**Total**
Acceptées	
Accès	378
Délais	437
Protection des renseignements personnels	1 458[1]
Total	**2 273**
Fermées au moyen du processus de règlement officiel	
Accès	107
Délais	114
Protection des renseignements personnels	78
Total	**299**
Fermées au moyen d'une enquête	
Accès	256
Délais	234
Protection des renseignements personnels	118
Total	**609**
Total des plaintes fermées	**908**

* Pour une description de chaque catégorie de plaintes, veuillez consulter l'annexe 1.

[1] Ce chiffre inclut 1 159 plaintes relatives à des atteintes à la vie privée concernant Ressources humaines et Développement des compétences Canada (appelé maintenant Emploi et Développement social Canada) acceptées au cours de l'exercice 2012 2013.

Examens des évaluations des facteurs relatifs à la vie privée

Reçues	**68**
Présentant un risque élevé	21
Présentant un risque faible	19
Total des évaluations examinées	**40**

Vérifications

Vérifications de la protection des renseignements personnels dans le secteur public déposées devant le Parlement	1

Politiques et affaires parlementaires

Ébauches de lois ou de projets de loi concernant le secteur public fédéral examinés sous l'angle de leurs répercussions sur la vie privée	8
Politiques ou initiatives du secteur public examinées sous l'angle de leurs répercussions sur la vie privée	51
Témoignages devant des comités parlementaires sur des enjeux touchant le secteur public	9
Présentations au Parlement	2
Autres interactions avec des parlementaires ou leur personnel (p. ex. la correspondance avec les députés ou les sénateurs)	52

Activités de communication *

Discours et exposés	88
Communiqués et autres outils de communication	27
Expositions et autres activités de promotion hors site	29
Publications distribuées	29 446
Visites sur le site Web principal du Commissariat	2,1 millions
Visites sur les blogues et autres sites Web du Commissariat	1,1 million

* Statistiques combinées concernant les initiatives des secteurs public et privé

Demandes soumises au Commissariat en vertu de la *Loi sur l'accès à l'information*

Demandes reçues	**50**
Demandes fermées	56

Demandes soumises au Commissariat en vertu de la *Loi sur la protection des renseignements personnels*

Demandes reçues	**17**
Demandes fermées	15

2.0 L'adoption de technologies de l'information vulnérables : Une période de risques croissants d'atteinte à la vie privée

Les Canadiennes et les Canadiens sont de plus en plus sensibles à la façon dont le gouvernement recueille et utilise leurs renseignements personnels. Lors du sondage téléphonique réalisé par le Commissariat en octobre et novembre 2012 auprès de 1 513 résidents adultes du Canada, les deux tiers ont déclaré être préoccupés par la protection de leurs renseignements personnels, et le quart d'entre eux, l'être « extrêmement ».

De plus, le sondage a révélé que les Canadiennes et les Canadiens ont de plus en plus l'impression que leur capacité de protéger leurs renseignements personnels diminue. Sept répondants sur dix pensent que leurs renseignements personnels sont moins protégés dans la vie de tous les jours qu'il y a dix ans, ce qui représente une augmentation de 10 % par rapport au résultat obtenu à la même question en 2011. Par ailleurs, seulement 21 % des répondants étaient d'avis que le gouvernement prend très au sérieux sa responsabilité de protéger les renseignements personnels des citoyens.

Le niveau de préoccupation du public au sujet de la protection de la vie privée a certainement augmenté encore davantage en janvier, lorsque Ressources humaines et Développement des compétences Canada (RHDCC)[2] a déclaré avoir perdu un lecteur de disque dur contenant les renseignements personnels de plus d'un demi-million de clients du Programme canadien de prêts aux étudiants. Une fois informé de cette atteinte, le Commissariat a entrepris une enquête et, au moment de la rédaction du présent rapport annuel, celle-ci suivait son cours.

[2] Ressources humaines et Développement des compétences Canada (RHDCC) a depuis été renommé Emploi et Développement social Canada. Toutefois, aux fins du présent rapport, nous utilisons le nom que portait le Ministère au moment des incidents et tout au long de la période visée par le rapport.

Une grave atteinte à la sécurité des renseignements personnels, comme la perte d'un lecteur de disque dur, est un exemple des vulnérabilités que présentent les technologies de l'information modernes en ce qui a trait à la protection de la vie privée. Selon le Commissariat, l'augmentation de ces vulnérabilités est l'une des quatre tendances qui contribuent à accroître le niveau d'inquiétude de la population canadienne à l'égard de la façon dont le gouvernement fédéral traite les renseignements personnels des citoyens. Des cas précis sont examinés plus loin dans ce chapitre.

Une deuxième tendance qui contribue au malaise croissant éprouvé par le public est la consultation inappropriée de renseignements personnels par des fonctionnaires, ce qui est mis en évidence au chapitre 3.

De plus, des éléments d'information indiquent que certains ministères et organismes gouvernementaux prennent de plus en plus de temps à répondre aux demandes d'accès aux renseignements personnels présentées en vertu de la *Loi sur la protection des renseignements personnels.* Dans certains cas, nous constatons aussi que des ministères et organismes gouvernementaux mettent plus de temps à répondre aux demandes d'information que nous leur soumettons dans le cadre d'enquêtes et d'autres affaires du Commissariat, une tendance inquiétante qui est décrite au chapitre 4.

La quatrième tendance pourrait bien être la plus difficile à contrer. Il s'agit de l'érosion continue de la protection de la vie privée de la population canadienne en raison des demandes constantes de renseignements personnels faites au nom de la sécurité nationale, au pays et à l'étranger. Le chapitre 5 traite en profondeur de cette question.

Malgré ces quatre tendances dérangeantes, la situation relative à la protection de la vie privée dans l'appareil fédéral n'est pas entièrement sombre. Comme nous l'indiquons dans les chapitres qui suivent, certaines institutions fédérales ont accompli des progrès dans le traitement en temps opportun des demandes présentées aux termes de la *Loi sur la protection des renseignements personnels*, et cela, bien que le nombre de demandes augmente sans qu'il y ait pour autant accroissement des ressources.

Par ailleurs, en ce qui a trait à l'analytique Web, qui soulève de nombreuses questions liées à la protection des renseignements personnels, le Commissariat a pu compter sur la coopération et la collaboration exemplaires de Services partagés Canada et du Secrétariat du Conseil du Trésor.

2.1 VULNÉRABILITÉ CONTINUE : LA GESTION DES RISQUES INTRINSÈQUES AUX TECHNOLOGIES DE L'INFORMATION

Les avantages sociaux associés à la technologie placent les citoyens dans une position paradoxale. Nous avons accès à l'information gouvernementale comme jamais auparavant, mais chaque nouvel appareil ou service électronique semble créer de nouveaux risques pour la protection de la vie privée. D'un côté, la grande quantité de renseignements personnels détenus par les ministères et les organismes fédéraux fait en sorte que, dans l'ensemble, la population canadienne reçoit des services efficaces dans tous les domaines, qu'il s'agisse des versements faits au titre du Régime de pensions du Canada (RPC) ou des remboursements d'impôt. Les gains d'efficience sont possibles parce que les bases de données sont exhaustives et largement accessibles aux organisations gouvernementales, et que les services publics sont instantanément disponibles en ligne.

D'un autre côté, cette collecte de données amplifie aussi les risques de chaos en cas d'erreur humaine ou d'une utilisation malveillante délibérée.

Les enquêtes réalisées par le Commissariat au cours du dernier exercice ont révélé que la vulnérabilité informatique était souvent associée à d'autres facteurs dans les cas où des institutions fédérales ne traitaient pas avec respect les renseignements personnels de la population canadienne.

Pour finir, la dernière année a été la troisième consécutive où le nombre d'atteintes à la sécurité des renseignements personnels signalées au Commissariat par les institutions fédérales a atteint un nombre record. Mentionnons notamment deux incidents signalés par RHDCC concernant la perte d'une clé USB contenant des renseignements personnels sensibles, dont les numéros d'assurance sociale et les renseignements sur l'état de santé de plus de 5 000 personnes, ainsi que d'un lecteur de disque dur contenant les renseignements personnels de plus de 500 000 bénéficiaires de prêts étudiants et de 250 employés du Ministère.

2.2 DIVULGATION DE RENSEIGNEMENTS OBTENUS PAR ÉCOUTE ÉLECTRONIQUE PAR LA GENDARMERIE ROYALE DU CANADA

Un autre cas de vulnérabilité informatique contribuant à l'érosion de la protection de la vie privée est présenté au chapitre 4. L'enquête de 32 mois, qui sert aussi d'exemple relatif aux délais pris pour donner suite aux demandes du Commissariat, portait sur la communication injustifiée, par la Gendarmerie royale du Canada (GRC), de renseignements personnels obtenus par écoute électronique autorisée par les tribunaux à un autre organisme gouvernemental.

Les renseignements concernaient un employé d'un organisme dont la conversation a été enregistrée alors qu'il parlait au téléphone avec une autre personne qui était sous écoute électronique par un service de police municipal. Ce dernier a transmis les renseignements obtenus par écoute électronique à la GRC, où l'employé de l'organisme était inscrit à un programme d'instruction des cadets.

La GRC a expulsé le cadet du programme et a remis les informations recueillies par écoute électronique à son employeur, ce qui constitue une infraction au *Code criminel* et, par ricochet, à la *Loi sur la protection des renseignements personnels.* L'organisme a congédié l'employé.

2.3 SERVICE CORRECTIONNEL DU CANADA

Un troisième exemple de vulnérabilités est lié à la gestion, par le Service correctionnel du Canada (SCC), des données contenues dans le Système de gestion des délinquants (SGD).

Le SGD est un système informatisé de gestion des cas qui est utilisé par le SCC et les autres intervenants du secteur de la justice criminelle pour gérer les renseignements sur les délinquants fédéraux tout au long de leur peine. Le système est utilisé pour recueillir, entreposer et extraire les renseignements nécessaires au suivi des délinquants et à la prise de décisions les concernant.

Divers renseignements personnels sur les délinquants sont conservés dans le SGD, notamment leurs antécédents criminels et les résultats de leurs évaluations psychologiques.

Un ex-détenu d'un établissement correctionnel à sécurité maximale s'est plaint au Commissariat du fait qu'on avait consulté son dossier sans raison valable et que certains de ses renseignements personnels avaient été communiqués aux médias sans son consentement.

Selon notre enquête, 98 personnes avaient consulté le dossier du plaignant dans le SGD au cours d'une période de presque cinq mois suivant sa mise en liberté, soit la période indiquée dans sa plainte. Deux de ces personnes, toutes deux des employés de l'établissement correctionnel, ont consulté le dossier du plaignant dans le SGD pour des raisons ne pouvant se justifier par le droit de savoir opérationnel.

Un employé a reconnu avoir consulté le dossier par curiosité. L'autre a déclaré avoir eu besoin d'obtenir plus d'information sur le plaignant pour sa propre sécurité et celle de sa famille.

En plus de ces cas d'accès inapproprié, notre enquête a aussi révélé plusieurs lacunes dans la gestion générale du SGD.

Par exemple, le SCC ne dispose actuellement d'aucune politique ou procédure traitant des responsabilités des superviseurs et des gestionnaires en ce qui a trait au signalement de tout accès inapproprié au SGD. En outre, l'organisme n'a pas mis en place de mesures de sécurité visant à surveiller

régulièrement l'accès au SGD et à repérer toute utilisation abusive de celui-ci.

Bien que le SCC reconnaisse la nécessité d'une mise à niveau et d'une mise à jour du SGD, aucune échéance n'a été établie pour l'examen initial.

Nous avons estimé que la plainte sur l'accès inapproprié était **fondée**. Toutefois, rien ne prouve que les deux employés ont communiqué les renseignements personnels diffusés par les médias.

2.4 RAPPORTS SUR LES ATTEINTES À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

Au cours du dernier exercice, nous avons assisté à une augmentation considérable du nombre d'atteintes à la sécurité des renseignements personnels signalées au Commissariat. Cela est attribuable soit à une hausse réelle du nombre d'incidents dans ce domaine au sein des ministères et des organismes fédéraux pour la troisième année consécutive, soit à une plus grande diligence de la part des institutions en matière de signalement des cas.

Étant donné que le signalement des atteintes à la sécurité des renseignements personnels est volontaire en vertu de la loi actuelle, il est impossible de connaître avec certitude l'incidence de chacun des facteurs sur cette hausse. Tout ce qu'on sait, c'est que 109 atteintes ont été signalées au cours du présent exercice comparativement à 80 au cours de l'exercice précédent.

Atteintes à la sécurité des renseignements personnels dans le secteur public fédéral signalées au Commissariat

2008-2009	26
2009-2010	38
2010-2011	64
2011-2012	80
2012-2013	109

L'ampleur, la complexité et les répercussions possibles de bon nombre de ces atteintes ont aussi augmenté, ce qui signifie que le Commissariat doit leur consacrer plus de temps, de ressources et d'efforts pour assurer le suivi approprié.

Une atteinte à la protection des données se produit lorsqu'il y a perte ou communication inappropriée de renseignements personnels. Les personnes touchées en sont informées ou non selon le niveau d'importance de l'atteinte. Il convient toutefois de souligner que, dans les deux grands incidents signalés cette année par RHDCC, on a avisé des centaines de milliers de personnes visées. De nombreuses personnes ont porté plainte au Commissariat.

Selon les lignes directrices du Secrétariat du Conseil du Trésor du Canada, les ministères et les organismes fédéraux sont invités — mais non contraints — à signaler rapidement au Commissariat toutes les atteintes graves à la sécurité des renseignements personnels. Six institutions fédérales étaient en cause dans près des deux tiers des incidents signalés. (Voir le tableau qui suit.)

Atteintes à la sécurité des renseignements personnels dans le secteur public fédéral signalées au Commissariat en 2012-2013

Ministère/organisme	Nombre d'atteintes signalées
Agence du revenu du Canda	22
Service correctionnel du Canada	17
Ressources humaines et Développement des compétences Canada	11
Affaires étrangères et Commerce international Canada[3]	10
Anciens Combattants Canada	5
Citoyenneté et Immigration Canada	5
Postes Canada	4
Statistique Canada	4
Défense nationale	3
Autres ministères ou organismes	28
Total	**109**

Comme ce fut le cas lors des exercices précédents, les communications accidentelles constituaient cette année la plus importante catégorie d'atteintes à la sécurité des renseignements personnels, soit 57 incidents essentiellement attribuables à une erreur humaine.

Treize atteintes concernaient l'accès non autorisé à des renseignements personnels ou la transmission non autorisée de documents. À ce nombre s'ajoutent 31 atteintes pouvant être attribuables à la perte de documents, dont six relatives à la perte de passeports à des ambassades du Canada.

[3] Le ministère des Affaires étrangères et du Commerce international (MAECI) a depuis été renommé le ministère des Affaires étrangères, du Commerce et du Développement; toutefois, aux fins du présent rapport, nous utilisons le nom que portait le Ministère pendant la période visée par le rapport.

Le vol de renseignements a été la cause de huit incidents. Les ordinateurs portables ont été une cible populaire comme l'indiquent, entre autres, les atteintes aux renseignements fiscaux personnels de 46 personnes et aux renseignements d'une douzaine de personnes ayant trait à l'examen en cours de leur situation relative au Régime de pensions du Canada et au programme de la sécurité de la vieillesse.

Deux atteintes à la sécurité des renseignements personnels ont beaucoup attiré l'attention des médias et ont conduit la commissaire à la protection de la vie privée à déposer des plaintes contre le ministère de la Justice Canada et RHDCC.

2.5 PERTE D'UNE CLÉ USB À RESSOURCES HUMAINES ET DÉVELOPPEMENT DES COMPÉTENCES CANADA ET AU MINISTÈRE DE LA JUSTICE CANADA

Ressources humaines et Développement des compétences Canada (RHDCC) a informé le Commissariat, le 6 décembre 2012, de la perte d'une clé USB contenant des renseignements personnels sensibles au sujet de plus de 5 000 personnes ayant porté en appel des décisions d'invalidité en vertu du Régime de pensions du Canada. Entre autres renseignements perdus concernant ces personnes, mentionnons leurs numéro d'assurance sociale (NAS), nom, date de naissance, état de santé, niveau de scolarité, profession ainsi que les noms de tous les autres organismes leur versant aussi des paiements, comme des indemnités d'accident du travail.

Nous avons par la suite été informés que la perte de la clé USB mettait en cause un avocat du ministère de la Justice Canada en poste à RHDCC. Le 28 janvier 2013, la commissaire a déposé une plainte contre le ministère de la Justice qui portait sur la perte des renseignements personnels stockés sur la clé USB.

Comme c'est la commissaire qui a déclenché le processus d'enquête, les 163 personnes qui avaient porté plainte contre RHDCC n'ont pas eu à déposer une plainte contre le ministère de la Justice pour que soit menée une enquête approfondie concernant le rôle de ce dernier dans l'incident de la perte de la clé USB. Les conclusions formulées par la commissaire à l'issue des enquêtes seront rendues publiques dès que ces dernières auront été achevées.

2.6 LA PERTE D'UN LECTEUR DE DISQUE DUR TOUCHE PLUS D'UN DEMI-MILLION DE BÉNÉFICIAIRES DE PRÊTS ÉTUDIANTS

RHDCC a informé le Commissariat de la perte d'un lecteur de disque dur externe contenant les renseignements personnels de 583 000 bénéficiaires de prêts étudiants et de 250 employés du Ministère. Les renseignements perdus comprenaient le NAS des clients, leur nom, leur date de naissance, leur adresse domiciliaire, leur numéro de téléphone et le solde de leur prêt.

La commissaire a déposé une plainte contre le Ministère le 11 janvier. Par conséquent, les personnes touchées n'ont pas eu à porter plainte individuellement pour qu'une enquête approfondie soit déclenchée. Néanmoins, au moment de rédiger le présent rapport, le Commissariat avait reçu 864 plaintes liées à cette atteinte. Les conclusions de la commissaire seront rendues publiques dès que l'enquête sera terminée.

RHDCC a écrit à quelque 310 000 bénéficiaires de prêts pour lesquels il avait des coordonnées à jour et exactes pour les informer de l'atteinte.

La commissaire à la protection de la vie privée entame une enquête concernant l'atteinte à la protection des renseignements personnels de bénéficiaires de prêts étudiants survenue à Ressources humaines et Développement des compétences Canada.
http://www.priv.gc.ca/media/nr-c/2013/an_130111_f.asp

2.7 SUIVIS IMMÉDIATS

Dans les deux cas, RHDCC a conclu un marché avec Equifax Canada et TransUnion afin d'offrir aux personnes touchées, avec leur consentement, des services de protection de l'identité et du dossier de crédit pendant une période maximale de six ans à la suite de l'incident.

Comme les clés USB et les lecteurs de disque dur externes sont grandement utilisés au sein de l'appareil gouvernemental, le Commissariat a décidé de procéder à une vérification d'autres organismes et ministères afin d'examiner leur utilisation des dispositifs de stockage portables.

2.8 VOL DANS UN VÉHICULE DE DOCUMENTS, D'UN ORDINATEUR PORTATIF CRYPTÉ ET D'UNE CLÉ USB APPARTENANT AU CENTRE D'ANALYSE DES OPÉRATIONS ET DÉCLARATIONS FINANCIÈRES DU CANADA

Le 18 octobre 2012, à Calgary, des documents papier, un ordinateur portable crypté et une clé USB contenant des renseignements liés aux examens du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) ont été volés dans un véhicule loué par un employé de l'organisme. Il semblerait que les documents contenaient des renseignements utilisés pour identifier des clients de casinos ainsi que des renseignements sur leurs opérations financières.

Selon l'enquête interne de CANAFE, une mesure de sécurité relative à l'utilisation des clés USB n'a pas été suivie. Quant à l'ordinateur portable, le lecteur de disque dur entièrement protégé est jumelé à l'ordinateur, ce qui signifie qu'il ne peut être décrypté qu'à partir de cet ordinateur portable et qu'il faut employer une combinaison de fonctions de sécurité pour avoir accès à l'information.

CANAFE a informé les personnes touchées par cette atteinte et revoit actuellement ses politiques et procédures concernant le transport et la sécurité de l'information. L'enquête sur l'atteinte à la sécurité des renseignements personnels survenue à CANAFE est en cours.

2.9 CLÉ USB NON CRYPTÉE DU SERVICE CORRECTIONNEL DU CANADA PERDUE ET RETROUVÉE DANS UNE COUR D'ÉCOLE

En déposant son enfant à l'école, un agent du renseignement de sécurité en poste à l'Établissement de Matsqui, qui est situé à Abbotsford, en Colombie-Britannique, a échappé une clé USB appartenant au Service correctionnel du Canada (SCC) dans la cour d'école. Un employé de l'école a trouvé la clé et, comme les lettres « CSC » (abréviation anglaise désignant le SCC) y figuraient, il l'a remise à un employé du SCC.

L'employé de l'école, tout comme l'employé du SCC qui a remis la clé USB à l'Établissement de Matsqui, ont affirmé ne pas avoir consulté le contenu de la clé USB non cryptée. Le dispositif contenait les renseignements personnels de 152 délinquants, y compris des renseignements sur des activités liées aux drogues et aux gangs.

Les représentants de l'équipe de la sécurité des technologies de l'information du SCC se sont engagés à envoyer un message de sensibilisation sur l'utilisation appropriée des clés USB à tous les employés de la région. Nous avons effectué un suivi pour nous assurer que cela avait bien été fait et nous sommes satisfaits des mesures mises en œuvre.

3.0 Manipuler avec soin :
Un appel au respect des renseignements personnels dans la foulée de nouveaux incidents liés à l'accès et à la collecte non autorisés

Les Canadiennes et les Canadiens s'attendent à ce que le gouvernement protège les grandes quantités de renseignements personnels qu'il détient contre la perte et l'accès non autorisé.

Pourtant, au cours du dernier exercice, le Commissariat a enquêté sur des fuites extrêmement graves de renseignements personnels placés sous la responsabilité du gouvernement, ainsi que sur des cas d'accès non autorisé à des renseignements personnels par des fonctionnaires — certains très haut placés — qui occupaient des postes de confiance. Certains des cas les plus troublants sont présentés dans ce chapitre.

Par exemple, nous décrivons la vérification d'une organisation habituée à en vérifier d'autres : l'Agence du revenu du Canada (ARC). Notre vérification a eu lieu après des années de rumeurs selon lesquelles des employés de l'ARC consultaient parfois les dossiers de contribuables sans y être autorisés.

Dans un sens, le gouvernement fédéral dépend totalement des recettes fiscales, dont le flux est facilité par les renseignements personnels. Nous estimons donc que le gouvernement fédéral devrait traiter les renseignements personnels avec tout le respect que les Canadiennes et les Canadiens attendent de sa part en ce qui a trait à la gestion des deniers publics.

Le présent chapitre porte aussi sur la collecte non autorisée, par Affaires autochtones et Développement du Nord Canada et Justice Canada, de renseignements personnels à partir de la page Facebook d'une militante pour les droits des Premières Nations. Notre enquête a permis de constater que les renseignements personnels recueillis par les ministères n'avaient aucun lien avec leurs programmes ou leurs activités et qu'ils ont, par conséquent, dépassé les limites, contrevenant ainsi à la *Loi sur la protection des renseignements personnels*.

3.1 VÉRIFICATION DE L'AGENCE DU REVENU DU CANADA

Contexte

Au cours des dernières années, le Commissariat a été informé de plusieurs atteintes à la vie privée particulièrement flagrantes mettant en cause l'Agence du revenu du Canada (ARC). Certaines de ces atteintes découlaient d'un mauvais acheminement du courrier, de la perte de dispositifs portables et d'une mauvaise utilisation du courriel.

Les atteintes les plus graves étaient le fait d'employés ayant consulté sans autorisation plusieurs dossiers de contribuables. Certaines d'entre elles sont passées inaperçues pendant plusieurs années avant d'être repérées et, dans un grand nombre de cas, les employés en cause ont utilisé abusivement des renseignements de contribuables à des fins personnelles ou pour en tirer un gain financier. Le Commissariat a été informé d'un petit nombre de ces atteintes par des plaignants, les médias ou l'ARC.

L'ARC est mise au courant de la plupart des atteintes à la vie privée par le public, par d'autres employés ou à la suite d'enquêtes internes. Elle l'est aussi, mais dans une moindre mesure, grâce à sa surveillance continue de l'accès des employés aux renseignements sur les contribuables. Les employés trouvés coupables d'avoir délibérément consulté ou divulgué des renseignements sur les contribuables peuvent faire l'objet de sanctions allant de la suspension sans solde au renvoi.

Une atteinte liée à la consultation ou à la communication de renseignements sensibles sur des contribuables peut avoir de graves répercussions sur la ou les personnes touchées. Dans le pire des scénarios, elle peut entraîner un vol d'identité, une fraude financière et un embarras personnel pour les contribuables visés. Les atteintes à la vie privée risquent aussi de ternir la réputation de l'Agence à titre de gardien de confiance des renseignements personnels sensibles des Canadiennes et des Canadiens.

À la lumière des questions qui ont été portées à l'attention du Commissariat, nous avons entrepris une vérification de l'ARC en 2012 aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels.* Notre objectif consistait à évaluer si l'Agence se conformait aux principes relatifs à l'équité dans le traitement de l'information énoncés dans la *Loi*. La vérification était axée sur les mesures de contrôle et de sécurité administratives et techniques en matière de consultation et de communication des renseignements contenus dans les systèmes de l'ARC sur les contribuables. Nous avons aussi examiné le cadre de l'Agence en ce qui a trait à la responsabilité et à l'évaluation de la menace en matière de protection de la vie privée, notamment à l'égard des éléments suivants : le leadership dans le domaine de la protection de la vie privée; la délégation des responsabilités; la formation et la sensibilisation des employés; les évaluations des facteurs relatifs à la vie privée (EFVP) et la gestion des atteintes à la vie privée. Enfin, nous avons passé en revue diverses

mesures visant à protéger les systèmes informatiques relatifs aux contribuables.

Le principe d'accès sélectif (accès en fonction du besoin de savoir) consiste à donner aux employés des privilèges d'accès seulement pour les dossiers et les renseignements personnels liés directement à leur description de travail, à leur affectation et à leur sphère de responsabilité. Ce principe devrait être au cœur de toute politique, pratique ou procédure régissant les privilèges d'accès des employés et leur exercice.

Par exemple, un commis à la saisie de données n'a pas besoin du même niveau d'accès aux systèmes qu'un vérificateur fiscal. De même, un vérificateur fiscal chargé des dossiers fiscaux d'entreprises ne devrait pas avoir régulièrement besoin d'accéder aux dossiers fiscaux de particuliers.

Il est essentiel de définir les privilèges d'accès des employés en fonction du principe d'accès sélectif si l'on veut assurer la protection des renseignements personnels de la population canadienne et se conformer aux exigences de la *Loi sur la protection des renseignements personnels*. Compte tenu de la nature des vastes activités de l'ARC, de son besoin de disposer de renseignements personnels sensibles sur les contribuables pour remplir son mandat, ainsi que des attentes élevées des Canadiennes et des Canadiens à l'égard de la protection de leurs renseignements personnels, nous nous attendions à constater que l'Agence avait mis en place de solides mesures de surveillance de l'accès afin de limiter le nombre et l'étendue des atteintes à la vie privée.

Points examinés

Lors de notre vérification de l'ARC de 2012, nous avons interviewé des employés de l'administration centrale et de centres fiscaux situés dans ses quatre principales régions — l'Ontario, le Pacifique, les Prairies et le Québec —, qui desservent plus de 80 % des contribuables canadiens.

Nous avons aussi examiné des documents clés, comme : les politiques et les procédures de l'Agence concernant les renseignements personnels, les sanctions disciplinaires et la sécurité; les documents de formation; les EFVP; les enquêtes sur les atteintes à la vie privée; les évaluations des menaces et des risques; les vérifications internes et les plans des risques organisationnels. Enfin, nous avons passé en revue les contrôles de sécurité des TI utilisés pour attribuer et mettre à jour les privilèges d'accès, surveiller l'accès des employés aux renseignements sensibles des contribuables, ou encore pour protéger les renseignements personnels de ces derniers.

Importance de l'enjeu

Depuis la diffusion d'un rapport de vérification en 2009, l'ARC a réalisé des progrès en ce qui a trait au renforcement de ses politiques et procédures en matière de sécurité et de protection de la vie privée, ainsi que dans la communication à ses employés de ses attentes à l'égard de la protection des renseignements personnels. Les fonds de renseignements personnels de l'ARC sont non seulement volumineux, mais aussi de nature très sensible. Les dossiers fiscaux des contribuables

contiennent en général des renseignements sur leur situation financière, leur état de santé, leur emploi et leur famille, de même que des renseignements permettant de les identifier. Les citoyens ne communiquent habituellement ces renseignements personnels qu'aux membres de leur famille et aux amis proches.

L'Agence a le mandat clair, en vertu de la *Loi de l'impôt sur le revenu*, de recueillir des renseignements auprès des Canadiennes et des Canadiens et de les utiliser à des fins d'administration fiscale. Cependant, il convient de rappeler que les données fiscales — déclarées tous les ans —n'appartiennent pas en fait à l'Agence, mais bien aux contribuables qui les fournissent.

L'Agence et ses 40 000 employés ont ainsi l'importante obligation juridique et éthique de veiller à prévenir la consultation, l'utilisation ou la communication inappropriées des renseignements personnels confiés à l'organisme par les Canadiennes et les Canadiens. Il faut respecter cette obligation quotidiennement et aussi longtemps que ces renseignements sont sous le contrôle juridique de l'Agence.

Année après année, l'ARC recueille des quantités impressionnantes de renseignements auprès de plus de 27 millions de contribuables canadiens. Ces renseignements constituent la fondation même sur laquelle repose notre régime fiscal. Pour que ce dernier fonctionne aussi efficacement qu'il le fait actuellement, l'Agence compte sur ces millions de contribuables qui transmettent des renseignements exacts, complets et opportuns et qui payent leurs impôts dans les délais prescrits. Selon la loi, les Canadiennes et les Canadiens sont tenus de produire leurs déclarations de revenus au plus tard à la fin avril de chaque année. Dans la pratique, l'ARC leur fait confiance pour qu'ils fournissent volontairement les renseignements demandés — sans qu'elle ait à intervenir. Quatre-vingt-onze pour cent des citoyens ont soumis à temps leurs déclarations de revenus en 2012. Ceux qui devaient des impôts les ont payés entièrement et dans les délais exigés dans une proportion de 94 %. Ce niveau de conformité extraordinaire de la part de la population canadienne ne devrait pas être pris à la légère.

Pour conserver l'inestimable et exceptionnel niveau de confiance et de bonne volonté des citoyens, il est essentiel que l'Agence continue de chercher à améliorer ses mesures de sécurité et de protection des renseignements personnels, et à réduire ses risques d'atteinte à la vie privée.

Constatations

L'ARC favorise une culture de sécurité et de confidentialité grâce à son cadre d'intégrité, ses politiques, sa formation, ses activités de sensibilisation et d'autres initiatives. Nous avons toutefois observé l'existence de lacunes de taille sur le plan de la mise en œuvre et de la surveillance de certaines de ses principales politiques et pratiques en matière de

sécurité et de protection de la vie privée. Ces lacunes nuisent à la capacité de l'ARC d'empêcher, dans la mesure du possible, la consultation, l'utilisation ou la communication inappropriées, à l'interne, de renseignements sur les contribuables. Nous avons plus particulièrement remarqué ce qui suit :

- Un chef de la protection des renseignements personnels a été nommé, trois ans après que l'ARC se soit engagée à le faire à la suite d'une recommandation découlant de notre vérification de 2009. Le rôle de ce dernier n'a cependant pas encore été pleinement défini de façon à assurer la coordination des obligations en matière de reddition de comptes, des responsabilités et des activités relatives à la protection de la vie privée à l'échelle de l'Agence;
- Une évaluation des facteurs relatifs à la vie privée (EFVP) n'est pas toujours menée à bien avant la mise en œuvre de changements à un programme susceptibles d'avoir des répercussions sur les renseignements personnels des contribuables;
- De nombreux systèmes informatiques traitant les renseignements des contribuables ne font pas l'objet d'une évaluation des menaces et des risques, ce qui pourrait empêcher de déceler des lacunes;
- L'efficacité des contrôles de l'Agence visant à prévenir et à détecter toute consultation et utilisation inappropriées de renseignements des contribuables par les employés, ainsi qu'à faire rapidement enquête sur ces derniers, est limitée par l'absence d'un outil automatisé qui repérerait et signalerait les potentiels cas d'accès inapproprié, et par certaines lacunes relatives à la collecte des données ayant trait aux pistes de vérification dans les systèmes informatiques de l'ARC;
- Des cas d'accès inapproprié aux dossiers de milliers de contribuables sont passés inaperçus pendant une longue période;
- Comme la Direction de l'accès à l'information et de la protection des renseignements personnels (DAIPRP) de l'Agence n'est pas informée de nombreuses atteintes à la vie privée résultant de la consultation et de la communication inappropriées de renseignements sur les contribuables, ces atteintes ne sont pas signalées au Commissariat, qui n'a pas l'occasion de fournir des conseils sur la façon d'éviter que d'autres atteintes semblables aient lieu.

Nos recommandations

Gestion et responsabilité en matière de protection de la vie privée

L'Agence devrait :

- définir pleinement le rôle du chef de la protection des renseignements personnels et surveiller la mise en œuvre de son mandat au chapitre de la sensibilisation des employés au respect de la vie privée, à la réduction du risque d'atteinte à la vie privée et au respect global de la *Loi sur la protection des renseignements personnels* à l'Agence;
- réaliser des EFVP, les examiner et les approuver avant la mise en œuvre de nouveaux programmes ou d'initiatives susceptibles d'augmenter les risques d'atteinte à la vie privée des contribuables;
- veiller à ce que sa Direction de l'AIPRP soit informée de toutes les atteintes dès qu'elles sont connues.

Accès des employés au système et surveillance de l'utilisation qui en est faite

L'Agence devrait :

- continuer d'accroître les contrôles de son système de gestion de l'identité et de l'accès afin de limiter l'accès des employés aux renseignements dont ils ont besoin dans l'exercice de leurs fonctions, selon le principe de l'accès sélectif;
- passer en revue les identificateurs d'utilisateur génériques[4] existants pour déterminer s'ils sont nécessaires, autorisés et s'ils font l'objet d'un contrôle, et supprimer tous les identifiants d'utilisateur génériques qui ne servent pas;
- veiller à ce que tous les identificateurs d'utilisateur génériques soient assujettis aux processus d'examen et d'approbation établis;
- continuer de renforcer ses systèmes et ses processus de consignation des vérifications et y intégrer des outils d'évaluation des risques de façon à être informée de toute activité inappropriée dans ses systèmes de la part du personnel;
- veiller à mettre en place des mesures suffisantes pour atténuer les risques associés à l'accès par les concepteurs aux renseignements de contribuables dans des environnements d'essai;
- contrôler les transferts de renseignements sur les contribuables de l'environnement opérationnel aux environnements d'essai[5], en assurer le suivi et les surveiller rigoureusement.

[4] Un identificateur d'utilisateur générique est un code dont se servent plusieurs personnes travaillant au même projet ou activité.

[5] Le personnel des TI a recours à des environnements d'essai non opérationnels pour élaborer et mettre à l'essai des systèmes avant qu'ils ne servent à traiter des déclarations de revenus dans le cadre des activités courantes, ou dans l'« environnement opérationnel », de l'Agence.

Sécurité des technologies de l'information

L'Agence devrait s'assurer :

- que ses politiques, pratiques et procédures en matière de gestion des applications locales sont suivies, et que des mesures de sécurité adéquates sont utilisées pour protéger les renseignements des contribuables que contiennent ces applications;
- que son référentiel des applications locales [6] est examiné périodiquement afin d'en vérifier l'intégralité, l'exactitude et l'actualité;
- qu'un suivi a lieu à chaque étape des processus d'examen et d'assurance de la qualité, et que toutes les applications locales sont approuvées par des employés autorisés avant d'être mises en œuvre.

Réponse de la direction de l'Agence du revenu du Canada à nos recommandations

L'Agence a accepté toutes nos recommandations et a répondu par un plan d'action concret et un calendrier d'exécution afin d'accroître ses mesures de sécurité et de protection de la vie privée de plusieurs manières importantes. Elle déploie également des efforts pour améliorer la gestion des droits d'accès et surveiller plus étroitement l'accès des employés aux renseignements des contribuables. Nous assurerons un suivi auprès de l'ARC dans deux ans afin de vérifier si elle a entièrement mis en œuvre tous les changements promis.

[6] Une application locale est un logiciel utilisé pour exécuter une fonction liée aux activités des technologies de l'information requises dans un emplacement local ou régional.

À propos de l'Agence du revenu du Canada

L'Agence du revenu du Canada (ARC) est assujettie à la *Loi sur la protection des renseignements personnels* et aux exigences en matière de sécurité et de protection des renseignements personnels du Secrétariat du Conseil du Trésor et du gouvernement du Canada en ce qui concerne la gestion et la protection des renseignements confidentiels de la population canadienne. L'article 241 de la *Loi de l'impôt sur le revenu* énonce aussi les exigences relatives aux renseignements confidentiels auxquelles les employés et toute autre personne ayant accès aux renseignements sur les contribuables doivent se soumettre. Des manquements graves à l'obligation de confidentialité à l'égard des renseignements des contribuables peuvent entraîner le congédiement d'un employé.

L'Agence est l'une des plus grandes institutions fédérales. Son mandat extrêmement vaste et complexe consiste à appliquer les lois fiscales, à percevoir les impôts et à verser de nombreuses prestations financières et économiques aux contribuables au nom du gouvernement fédéral et de la plupart des provinces et des territoires.

De toutes les organisations gouvernementales, l'ARC est celle qui interagit avec le plus grand nombre de Canadiennes et de Canadiens, et ses activités ont des répercussions considérables sur des millions de particuliers et d'entreprises. Elle détient aussi l'une des plus importantes bases de données au Canada.

En 2012, l'Agence a reçu près de 27 millions de déclarations de revenus, versé plus de 34 millions de dollars en paiements d'impôts, accordé 111 millions de dollars en crédits d'impôt et en prestations à quelque 12 millions de Canadiens, et répondu à 17,7 millions de demandes de renseignements de la part du public. De plus, la même année, son effectif comptait approximativement 40 000 employés répartis dans cinq régions, 40 bureaux des services fiscaux et centres fiscaux d'un bout à l'autre du pays. Environ deux de ces employés sur trois avaient un certain accès électronique aux renseignements des contribuables au moyen des divers systèmes de l'Agence.

Le commissaire et premier dirigeant de l'Agence voit à l'administration quotidienne des différents textes de loi, dont la *Loi de l'impôt sur le revenu* et la *Loi sur la protection des renseignements personnels*, ainsi qu'à leur respect. Toutefois, c'est le ministre du Revenu national qui est responsable en dernier ressort de l'observation des deux lois.

3.2 AFFAIRES AUTOCHTONES ET DÉVELOPPEMENT DU NORD CANADA RECUEILLE À TORT DES RENSEIGNEMENTS À PARTIR DE LA PAGE FACEBOOK PERSONNELLE D'UNE MILITANTE POUR LES DROITS DES PREMIÈRES NATIONS

L'idée fausse selon laquelle les gens renoncent à leur droit à la vie privée en affichant des renseignements à leur sujet sur Facebook semble malheureusement toujours circuler dans les milieux gouvernementaux.

Des fonctionnaires d'Affaires autochtones et Développement du Nord Canada (AADNC) et du ministère de la Justice Canada ont invoqué cet argument pour justifier leur collecte, depuis des années, de renseignements personnels affichés par la militante pour les droits des Premières Nations de premier plan, Cindy Blackstock, sur sa page Facebook personnelle.

À la suite d'une enquête officielle, le Commissariat a cependant rejeté l'argument. Nous avons conclu que le fait que des renseignements personnels soient accessibles sur Internet ne leur enlève pas leur caractère personnel.

Nous avons recommandé que les deux ministères cessent de consulter les renseignements personnels de M^me^ Blackstock qui sont affichés sur sa page Facebook et sur d'autres sites de médias sociaux, à moins qu'ils puissent démontrer que la consultation de ces renseignements est en lien direct avec des activités gouvernementales légitimes. Nous avons aussi recommandé la destruction des renseignements personnels recueillis antérieurement en l'absence d'un tel lien direct.

Enfin, nous avons recommandé à AADNC et au ministère de la Justice Canada d'établir et de mettre en œuvre des politiques et des lignes directrices internes régissant la collecte, par leurs employés, de renseignements personnels sur des sites de médias sociaux et la limitant aux renseignements ayant un lien direct avec leurs programmes ou activités.

Les deux ministères ont accepté toutes ces recommandations.

Contexte

M^me^ Blackstock a déposé une plainte au Commissariat dans laquelle elle affirmait que les deux ministères fédéraux avaient contrevenu à la *Loi sur la protection des renseignements personnels* en procédant à une collecte systématique et délibérée de ses renseignements personnels à des fins non liées directement à une activité ou à un programme gouvernemental.

La plainte portait plus précisément sur trois activités différentes :

- la surveillance furtive de ses discours publics et la distribution de rapports détaillés de ses commentaires à grande échelle dans les deux ministères;
- l'accès répété à son dossier de statut d'Indienne dans la base de données du gouvernement, même si personne ne mettait en doute ce statut;
- la consultation et la surveillance répétées de ses fils de nouvelles dans les médias sociaux, en particulier de sa page Facebook personnelle, et la distribution à grande échelle, au sein des deux ministères, de rapports sur l'information qu'elle avait affichée en ligne.

M^me^ Blackstock a aussi soutenu que ces atteintes à sa vie privée étaient liées à la poursuite judiciaire relative aux droits de la personne intentée contre le gouvernement fédéral par son employeur. Dans ce litige, on allègue que le financement inéquitable des services d'aide à l'enfance dans les réserves équivaut à de la discrimination.

Constatations

Après une enquête longue et approfondie, le Commissariat n'a tiré **aucune conclusion** sur la première activité, car, dans ce cas, l'information provenant des discours publics de la plaignante ne constituait pas des « renseignements personnels » aux termes de la *Loi sur la protection des renseignements personnels.* Nous avons jugé que la plainte à propos de la deuxième activité était **non fondée** en raison de l'absence de preuves.

Toutefois, nous avons conclu que la plainte ayant trait à la surveillance des médias sociaux était **fondée**.

En février 2010, les deux ministères ont commencé à surveiller les sites et les fils de nouvelles des médias sociaux liés à la plaignante, notamment Twitter, YouTube, BlogSpot, Alertes Google et trois pages Facebook distinctes administrées par la plaignante.

Notre enquête a révélé que deux des pages Facebook n'étaient pas de nature personnelle, mais plutôt consacrées essentiellement aux affaires de l'organisation des Premières Nations qui employait la plaignante, ainsi qu'à une campagne pour soutenir la plainte relative aux droits de la personne.

La troisième page, toutefois, avait été classée par Facebook comme une « page personnelle » et contenait de l'information sur les amis, les opinions personnelles, les compétences et le lieu de résidence de la plaignante, ce qui constitue clairement des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels.*

Selon notre enquête, les fonctionnaires des deux ministères savaient très bien qu'ils consultaient et compilaient des renseignements personnels sur la plaignante, et qu'ils ne se limitaient pas aux renseignements liés à son employeur ou à la campagne sur les droits de la personne. Aux termes de la *Loi*, des restrictions sur la collecte de

renseignements personnels s'appliquent, que ceux-ci soient accessibles au public ou non.

La principale restriction prévoit que les renseignements ainsi recueillis doivent être liés directement à un programme ou à une activité du gouvernement. Nous avons conclu dans notre enquête que les renseignements personnels recueillis ne présentaient pas de liens évidents avec l'élaboration de politiques par AADNC, comme l'affirmait le Ministère, ou avec la poursuite relative aux droits de la personne qui inquiétait beaucoup le ministère de la Justice.

De plus, le manque de transparence entourant la collecte de renseignements personnels sur la page Facebook de la plaignante par les deux ministères fédéraux semblerait contrevenir à l'esprit, sinon à la lettre, de la *Loi sur la protection des renseignements personnels*.

3.3 VÉRIFICATION DES ANTÉCÉDENTS CRIMINELS D'UNE LOCATAIRE

Une femme a demandé à louer un appartement situé au sous-sol d'un immeuble appartenant à deux employés de la Gendarmerie royale du Canada (GRC). Les propriétaires ont demandé des renseignements personnels afin de pouvoir « faire une vérification » des locateurs potentiels.

Pour accéder à cette demande, la femme a fourni son permis de conduire ainsi que celui de son colocataire.

Par la suite, la femme s'est plainte au Commissariat du fait que les propriétaires de l'immeuble avaient vérifié si elle avait un casier judiciaire en utilisant leur accès privilégié à la base de données nationale du Centre d'information de la police canadienne (CIPC).

Une enquête interne menée par la GRC a confirmé qu'un des propriétaires, un agent de la GRC, avait procédé à une vérification dans le système du CIPC sur la locataire potentielle parce qu'elle venait « de l'extérieur de la ville ». L'agent a indiqué avoir agi ainsi afin de réduire les risques pour la sécurité des agents et la sécurité organisationnelle.

Les renseignements contenus dans la base de données du CIPC constituent des renseignements personnels au sens de la *Loi sur la protection des renseignements personnels* et ils ne doivent, par conséquent, être utilisés qu'à des fins légitimes d'application de la loi, conformément aux politiques et aux procédures régissant l'utilisation de la base de données.

Notre enquête a révélé que l'agent de la GRC avait manifestement consulté la base de données pour des raisons personnelles, et non à des fins opérationnelles autorisées. Le 4 avril 2012, nous avons informé la GRC que la plainte était **fondée**.

Dans sa réponse du 30 avril 2012, la GRC a dressé la liste des mesures correctives prises :

- l'agent a été informé de la gravité de la situation et du caractère inapproprié de ses gestes;
- la GRC s'est excusée par écrit à la plaignante d'avoir enfreint son droit à la vie privée;

- le 20 avril, la GRC a diffusé un communiqué rappelant à tous les employés les politiques et les procédures régissant l'utilisation des bases de données de la GRC, dont celle du CIPC. Elle prévoyait aussi les informer, par voie de communiqués, des mesures qui seraient prises en cas de transgression.

Le Commissariat est satisfait de ces mesures correctives.

3.4 UNE FEMME ACCÈDE AUX DOSSIERS MÉDICAUX DE SON EX-MARI

Un sergent en poste dans une base des Forces canadiennes a déposé une plainte dans laquelle il affirmait que son ex-femme, qui travaillait comme civile à la base, avait consulté ses dossiers médicaux militaires sans son autorisation.

Le sergent a fourni une copie du rapport du registre de vérification du Système d'information sur la santé des Forces canadiennes (SISFC), qui indiquait quand son ex-femme avait consulté ses dossiers médicaux.

Le ministère de la Défense nationale (MDN) a confirmé que l'ex-conjointe avait consulté le compte du sergent dans le SISFC et qu'elle avait supprimé un rendez-vous de physiothérapie à son nom au Centre des services de santé de la base. Le Ministère nous a aussi informés que l'ex-femme avait été observée en train de consulter le dossier papier de physiothérapie du sergent, qui avait été placé dans une chemise de protection.

Étant donné que l'ex-épouse avait été bien informée des critères régissant une utilisation acceptable des dossiers électroniques du SISFC, le MDN a déterminé qu'elle avait sciemment contrevenu aux règles et règlements du Ministère. Il a automatiquement changé les paramètres régissant son accès au système afin de l'empêcher de consulter les dossiers médicaux du sergent dans le SISFC.

La consultation et l'utilisation des données médicales du sergent sont de toute évidence non conformes aux fins visées par la collecte initiale des renseignements et elles ne correspondent pas à l'un des critères d'utilisation permise définis dans la *Loi sur la protection des renseignements personnels.* Nous avons donc confirmé que la plainte était **fondée**.

Le MDN a indiqué au Commissariat qu'il avait mis en place de nouveaux contrôles dans le SISFC afin de composer avec les cas d'accès inapproprié. Il nous a aussi indiqué être en train d'évaluer les systèmes et les pratiques concernant la collecte, la conservation, l'utilisation et la communication des renseignements, ainsi que la sécurité générale des dossiers du SISFC.

3.5 ACCÈS NON AUTORISÉ À UN DOSSIER FISCAL PAR UN EMPLOYÉ DE L'AGENCE DU REVENU DU CANADA

Un plaignant a allégué que l'Agence du revenu du Canada (ARC) avait enfreint les dispositions sur l'utilisation et la communication des renseignements personnels contenues dans la *Loi sur la protection des renseignements personnels* lorsqu'un de ses employés avait consulté son dossier fiscal en 2005 et en 2006.

Le plaignant a commencé à se douter qu'on consultait son dossier fiscal lorsqu'il a découvert que plusieurs personnes appartenant à sa collectivité connaissaient des renseignements financiers le concernant, dont son salaire exact. Après avoir présenté à l'ARC une demande relative à ses renseignements personnels, il a reçu un rapport de vérification à rebours de son compte fiscal T1 montrant tous les accès à son dossier depuis plus de six ans.

En passant en revue ce rapport de vérification, il a reconnu le nom d'un employé de l'ARC qui avait consulté son dossier à deux reprises. Cet employé avait plus précisément eu accès aux renseignements personnels suivants à son sujet : numéro d'assurance sociale, revenus et déductions, feuillets de renseignements relatifs à l'emploi et aux revenus, historique des déclarations de revenus, renseignements sur les enfants, adresse, date de naissance et situation de famille.

Notre enquête a révélé que l'employé avait eu accès au compte sans autorisation et au-delà des pouvoirs et des exigences associés à son poste. Par conséquent, la plainte a été jugée **fondée**. L'ARC a confirmé que l'employé n'avait plus accès aux renseignements des contribuables.

3.6 ACCÈS, PAR UNE EMPLOYÉE DE LA DÉFENSE NATIONALE, AUX DOSSIERS DE SANTÉ D'UN INDIVIDU POUR DES RAISONS PERSONNELLES

Un plaignant a allégué que des renseignements personnels sur sa santé avaient été consultés de façon inappropriée par une employée des Forces canadiennes (FC) avec qui il avait entretenu une relation personnelle dans le passé.

Selon notre enquête, l'employée a consulté à plusieurs reprises les renseignements sur la santé du plaignant contenus dans le Système d'information sur la santé des Forces canadiennes (SISFC), après avoir reçu un message anonyme l'informant que le plaignant était « malade » et que, par ricochet, sa santé était en danger.

L'employée a admis avoir consulté et utilisé les renseignements confidentiels du plaignant pour des raisons personnelles, qui, clairement, étaient non conformes aux fins de la collecte; la plainte était donc **fondée**.

À la suite de notre enquête, le ministère de la Défense nationale (MDN) a reconnu l'importance d'un processus exhaustif et à jour sur la sensibilisation et la formation du personnel dans le domaine de la protection de la vie privée. Il nous a informés des mesures prises : la mise en œuvre de nouveaux contrôles dans le SISFC afin de composer avec les cas d'accès inapproprié; la mise à jour de la politique des Services de santé des Forces canadiennes sur l'utilisation et la communication appropriées de renseignements personnels sur la santé; la prestation d'une formation sur la protection de la vie privée des patients à l'intention du personnel de la santé des FC.

4.0 Justice différée est justice refusée :
Retards persistants de la part d'institutions fédérales à répondre aux demandes d'accès à des renseignements personnels présentées par des particuliers et aux enquêtes relatives aux plaintes du Commissariat

L'an dernier, nous avons sonné l'alerte concernant le trop grand nombre d'institutions fédérales qui, systématiquement, géraient mal les demandes d'accès des Canadiennes et des Canadiens à leurs renseignements personnels. Cette année, la tendance des retards croissants s'est poursuivie et même accentuée.

Le nombre de plaintes relatives aux retards a été élevé de façon constante ces dernières années, mais il a été sans précédent en 2012-2013. Les demandes se sont aussi complexifiées et bon nombre d'entre elles concernent l'accès aux courriels, ce qui rend le processus plus ardu pour les institutions fédérales.

Nous avons aussi remarqué l'apparition d'une tendance dans certaines institutions, soit la perte de l'expertise entourant le processus d'examen, ce qui a pour effet d'entraîner d'autres retards. En outre, comme les institutions doivent répondre à un nombre accru de demandes d'accès à des renseignements personnels, elles prennent encore plus de temps à donner suite aux demandes du Commissariat.

Pour que le droit à la vie privée garde tout son sens, les organisations doivent veiller à respecter leurs obligations, et ce, en temps opportun. Malheureusement, les institutions fédérales continuent d'éprouver des difficultés à répondre aux demandes de renseignements personnels dans les délais prévus par la loi, échouant de plus en plus à ce chapitre.

Aspect tout aussi important, elles ont du mal à répondre en temps opportun au Commissariat après le dépôt d'une plainte. Cela se traduit souvent par des enquêtes plus longues et qui nécessitent davantage de ressources.

Bref, s'il est vrai que le temps, c'est de l'argent, la population canadienne est perdante sur les deux plans. En voici quelques exemples.

4.1 GENDARMERIE ROYALE DU CANADA

Un plaignant a déposé de multiples plaintes pour refus d'accès à l'endroit de la Gendarmerie royale du Canada (GRC). En raison d'une erreur, la GRC n'a pas traité certaines demandes, ce qui a causé d'autres délais. De plus, l'enquête a pris du retard, car le responsable de la liaison administrative désigné par la GRC n'était pas familier avec les demandes, ce qui l'a forcé à transmettre les questions demandant des éclaircissements à un analyste au fait des dossiers.

La collaboration non coordonnée de la part de la GRC a occasionné des retards prolongés tout au long de l'enquête, ce qui a contribué à la difficulté de repérer des documents. Par exemple, dans le cadre d'une enquête sur un document manquant, le Commissariat a demandé une copie d'un présumé document manquant (un cahier d'information) pour déterminer si ce dernier était pertinent. La GRC a mis 15 mois pour fournir le cahier, en partie en raison de vues divergentes sur ce qui constituait des documents pertinents dans le cadre de la demande, mais aussi parce que la recherche du document avait pris beaucoup de temps.

Voici un autre cas relatif à la GRC : un individu s'est plaint que l'organisme avait enfreint son droit à la vie privée en communiquant des renseignements personnels le concernant à son employeur d'alors sans autorisation légale. À la lumière de cette information, le plaignant a été expulsé d'un programme d'instruction des cadets de la GRC et, par la suite, son employeur l'a congédié.

***Un accès retardé est un accès refusé : Information destinée aux responsables de l'accès à l'information et de la protection des renseignements personnels sur les demandes d'accès réputées refusées en vertu de la* Loi sur la protection des renseignements personnels**

Une grande majorité des plaintes reçues au Commissariat proviennent d'individus alléguant qu'une institution fédérale aurait, de manière injustifiée, refusé de leur communiquer des renseignements personnels les concernant dans les délais prévus.

La *Loi sur la protection des renseignements personnels* confère aux individus le droit général d'accéder, sur présentation d'une demande écrite, aux renseignements personnels les concernant qui sont détenus par les institutions fédérales. Bien qu'il existe des exceptions, les institutions fédérales sont, de manière générale, obligées de donner suite à ces demandes.

Le Commissariat a élaboré de l'information sur ce processus et les efforts qu'il déploie pour accélérer le cours des choses.

http://www.priv.gc.ca/resource/fs-fi/02_05_d_50_f.asp

Les renseignements personnels en question avaient été obtenus lors d'une opération d'écoute électronique autorisée par les tribunaux par un service de police municipal qui menait une enquête sur une autre personne ayant commis des actes criminels. Pour

de plus amples renseignements sur le contenu de cette affaire, on peut se reporter au chapitre 2. Par ailleurs, l'affaire montre bien les retards importants attribuables à un ministère fédéral.

Tout au long de ce long processus, la GRC a avancé au moins six arguments juridiques distincts pour justifier la communication des renseignements obtenus par écoute électronique. Lorsque le Commissariat a posé des questions ou demandé qu'on lui fasse d'autres observations concernant chaque argument, la GRC s'est souvent contentée de répondre en invoquant un autre argument juridique sans lien avec la question.

En résumé, la durée de 32 mois de cette enquête est attribuable en grande partie aux retards injustifiés occasionnés par la GRC.

4.2 RETARDS DANS LA COMMUNICATION D'UNE RÉPONSE AUX DEMANDES D'ACCÈS

La tendance à la hausse en ce qui a trait au nombre de plaintes relatives à des retards devrait se poursuivre, car les institutions ont du mal à donner suite aux demandes de renseignements personnels dans les délais prescrits.

Voici quelques cas alarmants que nous avons observés.

Transports Canada : Dans trois cas distincts, le Ministère a pris 21, 23 et 27 mois pour traiter la demande. Dans un cas, le retard était attribuable à un manque de personnel détenant la cote de sécurité appropriée pour examiner les documents.

Gendarmerie royale du Canada : Le nombre de plaintes relatives aux délais à la Gendarmerie royale du Canada (GRC) a grandement augmenté — 96 cette année par rapport à 25 l'an dernier. En 2012-2013, nous avons constamment reçu en retard les renseignements demandés à la GRC, ce qui a considérablement diminué notre capacité de mener nos enquêtes en temps opportun.

Lorsque la GRC répondait finalement à une demande (habituellement dans un délai de 8 à 12 mois — si celle-ci ne portait pas sur de nombreux documents), le Commissariat n'était généralement pas tenu au courant de l'avancement du traitement de la demande, à moins d'assurer lui-même le suivi. Dans l'ensemble, la GRC semblait avoir une piètre compréhension du processus d'enquête et du mandat du Commissariat, quand ce n'était pas carrément du mépris à notre égard. Nous constatons toutefois qu'au moment de rédiger le présent rapport, la GRC avait pourvu des postes clés au sein de son Bureau de l'accès à l'information et de la protection des renseignements personnels. Nous espérons qu'il en découlera des résultats plus positifs au cours du prochain exercice. Nous surveillerons la situation de près.

Ministère de la Justice Canada : Les retards de ce ministère ont été si importants que nous avons activement cherché à accélérer l'adoption de mesures concernant trois demandes d'accès réputées refusées au cours du dernier exercice. Le Ministère avait fourni des plans de travail précisant quand il aurait terminé le traitement des plaintes mais il ne les a pas respectés. Le Commissariat a présenté des demandes distinctes à la Cour fédérale au sujet de deux des plaintes, mais lorsque le Ministère a finalement envoyé les derniers documents aux plaignants, le Commissariat a abandonné les demandes, car la question du respect des délais était alors devenue sans objet. Quant à la troisième plainte, l'auteure de celle-ci n'a pas consenti à ce que nous présentions une demande en son nom.

Service correctionnel du Canada : Cet organisme continue d'afficher le plus grand nombre de plaintes relatives aux délais. Il convient cependant de noter que le mode de traitement des demandes adressées au Service correctionnel du Canada (SCC) a tendance à donner lieu à un nombre élevé de plaintes. Par exemple, si une demande nécessite la consultation d'un certain nombre de fichiers de renseignements personnels, SCC la traite comme s'il s'agissait de plusieurs demandes et la déclare ainsi, ce qui peut accroître le nombre de retards.

Malgré le nombre record de plaintes relatives aux délais déposées à son endroit, SCC s'efforce de collaborer avec nous, de nous fournir des plans d'action et des dates d'engagement, et de nous répondre rapidement.

Exemple de réussite — Défense nationale : Bien qu'il reçoive depuis quelques années un nombre beaucoup plus grand de demandes, le ministère de la Défense nationale (MDN) a réussi à trouver des façons efficaces de diminuer le temps nécessaire pour y donner suite. Le nombre de plaintes relatives aux délais reçues au Commissariat au sujet du MDN a considérablement diminué, passant de 77 en 2011-2012 à 52 en 2012-2013. De plus, le Ministère entretient une très bonne relation de collaboration avec le Commissariat ainsi que d'excellentes communications.

5.0 Confidentialité et sécurité :
Garantir le droit à la vie privée dans un contexte de renforcement de la sécurité publique

Les questions entourant la sécurité publique ont, pour des raisons évidentes, occupé de nombreux spécialistes des politiques et alimenté maintes discussions tout au long des premières années du 21e siècle. S'il est indéniable que la sécurité représente une responsabilité pour le gouvernement et un besoin pour les êtres humains, il en va de même de la protection de la vie privée. Il est impossible d'en abandonner indûment l'une au profit de l'autre, et c'est là que réside la difficulté de mettre de l'avant des mesures visant à renforcer la sécurité publique tout en respectant et en protégeant la vie privée de la population canadienne. Les paragraphes qui suivent portent sur divers aspects de cet enjeu.

Nous présenterons tout d'abord les résultats de la vérification du Commissariat concernant le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), qui reçoit quotidiennement 65 000 déclarations sur les opérations financières des Canadiennes et des Canadiens en provenance de banques, d'agents d'assurance-vie, d'agents immobiliers et de casinos. Notre vérification a révélé que CANAFE recueillait et conservait des renseignements personnels au-delà des limites autorisées en vertu de la loi applicable. De plus, l'organisme n'a pas encore mis fin à cette pratique.

Le présent chapitre porte également sur la forme la plus récente prise par le débat sur l'accès légal ainsi que sur les efforts que nous avons déployés en vue d'établir un dialogue avec les institutions fédérales au sujet de leur utilisation possible de véhicules aériens sans pilote.

Il présente aussi de façon détaillée des initiatives importantes liées au plan d'action *Par-delà la frontière*. Dans l'intention déclarée d'accroître la sécurité et de faciliter le flux des échanges commerciaux, le Canada et les États-Unis mettent actuellement en place des mesures le long de leur frontière commune. Bon nombre de ces mesures ont trait aux déplacements des gens et sont susceptibles d'avoir des répercussions de taille sur la protection de la vie privée. Dans les exemples fournis dans ce chapitre, mentionnons celui de la fouille à nu potentielle de toute personne entrant dans certaines zones situées près de la frontière ou associées à celle-ci, même si aucun panneau n'annonce de telles zones.

5.1 VÉRIFICATION DU CENTRE D'ANALYSE DES OPÉRATIONS ET DÉCLARATIONS FINANCIÈRES DU CANADA

Le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) est un organisme fédéral indépendant autorisé à recevoir et à analyser des données sur des opérations financières, et à diffuser des renseignements relatifs à des activités présumées de blanchiment d'argent et de financement du terrorisme.

Le Centre, qui a été créé en 2001, mène ses activités indépendamment des organismes d'application de la loi, mais peut communiquer des renseignements à ces derniers, aux organismes de sécurité, à l'Agence des services frontaliers du Canada et à l'Agence du revenu du Canada.

Plus de 300 000 entités sont tenues par la loi de déclarer les opérations importantes en espèces et les télévirements de 10 000 $ ou plus de leurs clients. Toutes les opérations —ou les tentatives d'opérations — pour lesquelles il existe des « motifs raisonnables de soupçonner » un lien avec des activités de blanchiment d'argent ou de financement du terrorisme, et ce, quel que soit le montant en cause, doivent être déclarées.

Les rapports sont soumis sans le consentement des clients et la plupart du temps sans qu'ils en aient connaissance. Dans le cadre de cette surveillance financière, CANAFE reçoit plus de 65 000 déclarations par jour (principalement de la part d'institutions financières), décrivant les opérations financières privées des citoyens ordinaires. Compte tenu des risques évidents d'atteinte à la vie privée, les Canadiennes et les Canadiens doivent être assurés que leurs renseignements personnels sont gérés de façon appropriée conformément aux mesures de contrôles établies. La protection de la vie privée consiste non seulement à protéger les données, mais aussi à veiller à ce que seuls les renseignements personnels strictement nécessaires sont recueillis et conservés.

En vertu des modifications adoptées en 2006, la loi régissant CANAFE — la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* — exige que le Commissariat procède à un examen de CANAFE tous les deux ans et en présente les résultats au Parlement. Notre première vérification a été menée à bien en 2009.

Points saillants de notre vérification de 2009

En 2009, nous avons constaté que CANAFE avait reçu et conservé des renseignements personnels dans une mesure outrepassant sa compétence législative. CANAFE devait améliorer ses mécanismes de contrôle, y compris l'examen préliminaire et la surveillance continue des déclarations, de manière à ce que ses fonds de renseignements soient pertinents sans être excessifs.

Malgré la mise en place de certains éléments d'un cadre de gestion de la protection de la vie privée, CANAFE devait corriger certaines lacunes. Nous

avons aussi constaté que CANAFE était incapable de fournir l'assurance que les directives transmises par ses partenaires du domaine de la réglementation aux entités déclarantes étaient conformes aux exigences établies dans la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*.

Objet de la plus récente vérification

Cette année, nous avons effectué une vérification axée sur l'évaluation des progrès réalisés par CANAFE dans la mise en œuvre des recommandations formulées en 2009. Nous avons aussi examiné la gestion des renseignements personnels acquis, utilisés et communiqués par CANAFE en sa qualité d'unité du renseignement financier et aussi dans le cadre de l'exercice de son mandat de conformité.

Constatations

Bien que CANAFE ait initialement réagi positivement à 10 des 11 recommandations de la vérification précédente, et qu'il ait accepté d'adopter des mesures pour corriger les lacunes et les faiblesses observées, nous avons constaté pendant la vérification que l'organisme a accompli des progrès limités pour donner suite à la moitié des recommandations.

La vérification de 2009 a permis de mettre en lumière certains secteurs où CANAFE pourrait renforcer les mesures de protection de la vie privée de la population canadienne. Par exemple, nous avons recommandé que l'organisme collabore avec ses partenaires du secteur des renseignements pour s'assurer, dans la mesure du possible, que toute affiliation de personnes avec des groupes terroristes soit confirmée avant de conserver ces données et de les rendre disponibles à des fins d'analyse. Nous avions aussi recommandé que CANAFE établisse par écrit des critères qui aideraient les responsables devant soumettre des rapports à l'Agence des services frontaliers du Canada et au Centre de la sécurité des télécommunications Canada à déterminer quand ont été atteints les seuils de communication. Des progrès satisfaisants ont été enregistrés pour donner suite à ces recommandations.

Dans la même veine, CANAFE a fait des progrès satisfaisants pour combler les lacunes décelées dans son cadre de gestion de la protection de la vie privée. Pour donner suite à la recommandation formulée à l'issue de la vérification de 2009, l'organisme a :

- nommé un chef de la protection des renseignements personnels chargé d'assurer un leadership stratégique et de surveiller les activités liées à la protection de la vie privée;
- établi un processus officiel pour recenser et atténuer les risques d'atteinte à la vie privée associés aux nouveaux programmes et services, ou à ceux qui ont été restructurés en profondeur;
- mis en œuvre un protocole de détermination et de signalement des atteintes à la vie privée;
- élargi les initiatives de sensibilisation à la sécurité.

Bien que CANAFE ait amélioré son processus de gestion des évaluations des menaces et des risques et qu'il continue d'avoir une infrastructure de sécurité

robuste, nous avons trouvé des cas de non-respect des politiques établies en matière de sécurité.

Déclarations excessives

Certaines des plus importantes lacunes relevées dans notre vérification précédente avaient trait à la réception et à la conservation de renseignements personnels. En 2009, nous avons constaté que les entités déclarantes communiquaient à CANAFE des renseignements dans une mesure qui dépassait les exigences énoncées dans la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, au sujet notamment :

- d'opérations financières sous le seuil de déclaration de 10 000 $;
- de déclarations d'opérations douteuses qui ne démontraient pas de « motifs raisonnables de soupçonner » des activités de blanchiment d'argent ou de financement du terrorisme;
- de déclarations de renseignements transmis volontairement où les soupçons d'activités de blanchiment d'argent ou de financement du terrorisme n'apparaissent pas clairement.

Nous avons recommandé, en 2009, que CANAFE prenne des mesures pour limiter la réception de renseignements personnels à ceux exigés par la loi. Acceptant cette recommandation, l'organisme a déclaré qu'il avait déjà adopté des mesures afin d'atténuer le risque de recevoir des renseignements qui n'auraient pas dû lui être envoyés. Malgré cet effort, la déclaration excessive est toujours un problème.

Dans un échantillon de rapports examinés au cours de la présente vérification, nous avons relevé un certain nombre de déclarations d'opérations importantes en espèces, de rapports de télévirements internationaux et de rapports sur le mouvement transfrontalier d'espèces monétaires concernant des sommes inférieures au seuil de déclaration de 10 000 $. Nous avons aussi relevé des cas de déclarations ne reposant pas sur des soupçons fondés; ces déclarations ne démontraient pas clairement l'existence de motifs raisonnables de soupçonner des activités de blanchiment d'argent ou de financement du terrorisme. En voici quelques exemples :

- Un jeune professionnel a encaissé trois traites bancaires d'une valeur de près de 100 000 $ US achetées dans une grande banque canadienne. Celle-ci a confirmé la validité des traites. Le gestionnaire de l'entreprise de services monétaires où les traites ont été encaissées a obtenu des réponses satisfaisantes aux diverses questions posées au sujet de l'opération, mais il a néanmoins déposé une déclaration d'opération douteuse en expliquant que la « somme d'argent était tout simplement incompatible avec l'âge du jeune homme ».
- Une personne, qui a acheté la maison d'un ami d'enfance, a remis le dépôt directement au vendeur plutôt qu'à l'avocat du vendeur. Le notaire qui a signalé l'opération a fourni l'explication suivante : « Il s'agit d'un de mes clients de longue date et je n'ai aucune raison de soupçonner du blanchiment d'argent ou des activités terroristes, mais comme je n'étais pas certain s'il fallait déclarer ou pas ce genre

d'opération (décrite ci-dessus), j'ai pensé qu'il était préférable de la déclarer. »

- Une personne voulait changer 5 000 euros en dollars canadiens. Pour l'en dissuader, l'entité déclarante l'a informée que le montant serait gelé en entier pendant 21 jours. Le client a décidé de ne pas effectuer la transaction.

Ces exemples pourraient donner à penser que certaines entités déclarantes ne connaissent toujours pas bien leurs obligations en matière de déclaration, ou qu'elles choisissent de déclarer en cas de doute, faisant de la protection de la vie privée une considération secondaire.

Il est essentiel, pour protéger la vie privée, de conserver uniquement les renseignements personnels pour lesquels il existe un besoin légitime et autorisé. En 2009, nous avions recommandé à CANAFE de supprimer définitivement de ses fonds de renseignements toutes les données qu'il n'aurait pas dû recevoir. L'organisme a bien accueilli la recommandation, reconnaissant l'importance de veiller à ce que sa base de données ne contienne que des renseignements qu'il est autorisé à détenir. Il a déclaré qu'il continuerait à chercher et à mettre au point de nouvelles façons d'atteindre cet objectif.

Malheureusement, CANAFE a accompli peu de progrès en ce qui a trait au respect de cet engagement. Il continue de conserver des renseignements qui ne respectent pas les paramètres et les seuils des opérations à déclarer indiqués dans la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*. Le fait de rendre accessibles des renseignements qui n'auraient jamais dû être recueillis au départ constitue un risque indiscutable d'atteinte à la vie privée.

Nos recommandations

Un grand nombre des recommandations formulées à l'issue de la vérification de 2013 sont semblables à celles formulées en 2009.

Pour que CANAFE puisse concilier ses obligations aux termes de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* avec celles découlant de la *Loi sur la protection des renseignements personnels,* nous lui recommandons d'analyser et d'évaluer les déclarations reçues afin de s'assurer qu'il ne conserve que les renseignements que la loi l'autorise à recevoir et qui sont liés directement à un programme ou à une activité. À titre de mesure complémentaire, nous recommandons à CANAFE d'évaluer l'efficacité de ses programmes de sensibilisation et de les renforcer au besoin afin d'atténuer le risque de signalement excessif de la part des entités déclarantes.

Nous avons aussi réitéré notre recommandation de 2009, dans laquelle nous demandions à CANAFE de repérer et d'éliminer les renseignements personnels qu'il détient actuellement et qu'il n'aurait pas dû recevoir, et qui n'ont pas de lien direct avec ses programmes ou activités.

Nous ne savons pas dans quelle mesure la base de données de CANAFE contient des renseignements que l'organisme ne devrait pas conserver.

Autres enjeux — Mandat de conformité

En plus de ses fonctions d'analyse et de communication, CANAFE a le mandat de veiller à ce que les entités déclarantes se conforment à leurs obligations en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*. Il remplit ce mandat de diverses façons, notamment par la réalisation d'examens de conformité dans le cadre desquels il recueille et examine les renseignements personnels des clients des entités déclarantes.

La limitation de la collecte de renseignements personnels, ou la réduction au minimum de la quantité de données recueillies, est un élément clé de la protection de la vie privée. La réduction au minimum de la quantité de données recueillies — limiter la collecte de renseignements à ce qui est strictement nécessaire à une fin déterminée — diminue les risques d'atteinte à la vie privée. En termes simples, des données non recueillies sont des données qui ne risquent pas de faire l'objet d'une atteinte à la vie privée.

Au cours de notre vérification précédente, nous avons repéré des cas où la conservation par CANAFE de certains types de documents n'était pas justifiée pour l'exécution de sa fonction de conformité. Nous avons remarqué que certains dossiers d'examen de l'organisme contenaient des renseignements personnels très détaillés qui ne semblaient pas nécessaires pour justifier les constatations des examens.

Nous avons alors recommandé que CANAFE respecte le principe de réduction au minimum de la quantité de données recueillies. L'organisme s'est dit en accord avec la recommandation et a affirmé qu'il insisterait sur l'importance de respecter ce principe dans le cadre de la formation donnée à ses agents de vérification de la conformité, et lors de la mise à jour de ses politiques et procédures.

En juin 2009, CANAFE a établi une politique en vertu de laquelle tous les documents obtenus au cours d'un examen de conformité sont numérisés et conservés en format électronique; quant aux copies papier, elles sont détruites. En raison du nombre accru d'examens, le personnel responsable de la conformité a reçu la directive, en 2011, de limiter la numérisation et la conservation aux documents nécessaires pour étayer les lacunes sur le plan de la conformité.

Notre dernière vérification nous a cependant permis de constater que CANAFE n'avait pas mis à jour ses politiques et procédures afin de rendre officiellement compte de la directive de 2011. De plus, il ne s'est pas doté de critères ou de lignes directrices pour aider les agents de vérification de la conformité à déterminer le type de documents ou de renseignements qui sont pertinents pour corroborer les lacunes en matière de conformité.

Nous avons également observé un manque d'uniformité dans l'application de la politique de numérisation, ainsi que dans la collecte et la reproduction d'identifiants personnels (p. ex. le numéro d'assurance sociale et celui de la carte santé). Nous avons aussi trouvé des cas où les dossiers

de conformité contenaient des renseignements personnels non requis pour étayer les résultats d'examen.

Réponse de CANAFE

Nous avons formulé neuf recommandations à l'intention de CANAFE dans la foulée de notre vérification de cette année. CANAFE les a toutes acceptées et a indiqué que des mesures adéquates étaient déjà en place pour donner suite à cinq d'entre elles. Nous croyons cependant qu'il reste du travail à faire. L'organisme a accepté de mettre en place des mesures pour donner suite aux quatre autres recommandations.

CANAFE a déclaré qu'il acceptait nos recommandations actuelles visant à limiter la collecte et la conservation des renseignements personnels qui dépassent les paramètres et les seuils des opérations à déclarer en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*. Malgré son adhésion à des recommandations semblables en 2009 et son engagement à les appliquer, l'organisme soutient maintenant qu'il est légalement tenu de recevoir et de conserver pendant dix ans les déclarations ou les renseignements fournis par les entités déclarantes, et ce, même si ces déclarations ou ces renseignements portent sur des opérations qui ne satisfont pas aux paramètres et aux seuils établis par la loi.

Conclusion

CANAFE a affirmé qu'il avait l'obligation, en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes,* de recevoir et de conserver les déclarations ou les renseignements fournis, et ce, que les déclarations ou les renseignements portent sur des opérations visées par la loi ou pas. Or, l'article 4 de la *Loi sur la protection des renseignements personnels* exige que les institutions fédérales limitent la collecte de renseignements à ceux qui ont un lien direct avec un programme ou une activité.

En d'autres mots, les institutions ne devraient pas recueillir ou conserver de renseignements, sauf si ces derniers sont requis pour leur permettre de remplir leur mandat. De plus, selon la politique du Secrétariat du Conseil du Trésor, elles doivent démontrer qu'elles ont besoin de chaque renseignement personnel recueilli pour réaliser le programme ou l'activité indiqué.

La *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* oblige CANAFE à analyser et à évaluer les déclarations qu'il reçoit. CANAFE a déclaré que son obligation à cet égard consiste à analyser et à évaluer les déclarations afin de déterminer s'il convient de communiquer l'information à ses partenaires de l'application de la loi ou de la sécurité dans le cadre de la communication de renseignements financiers.

CANAFE soutient aussi qu'il est légalement tenu de conserver tous les renseignements qu'il reçoit

pendant au moins dix ans, quelle que soit leur pertinence.

Cependant, il doit concilier la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* avec les exigences de la *Loi sur la protection des renseignements personnels*. Pour y arriver, l'organisme doit également analyser et évaluer les déclarations afin de s'assurer de ne pas accepter ou conserver de renseignements en dehors des paramètres et des seuils définis dans la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*. Tant qu'il n'aura pas mis en place un processus à cette fin, CANAFE continuera de recevoir et de conserver des renseignements dont il n'a pas besoin ou dont il ne se sert pas dans le cadre des ses programmes ou de ses activités; par extension, il ne respectera donc pas les obligations qui lui incombent aux termes de la *Loi sur la protection des renseignements personnels*.

Entités déclarant des renseignements personnels à CANAFE

- Toutes les catégories d'entités financières (banques, coopératives de crédit, caisses populaires);
- Les compagnies, les courtiers et les agents d'assurance-vie;
- Les courtiers en valeurs mobilières, les gestionnaires de portefeuille et les conseillers en placements autorisés par les provinces;
- Les courtiers de change;
- Les entreprises de services monétaires;
- Les négociants en métaux précieux et en pierres précieuses;
- Les mandataires de Sa Majesté qui acceptent les passifs-dépôts ou vendent des mandats;
- Les comptables/cabinets d'experts comptables et les courtiers/agents immobiliers qui participent à des activités comme la réception et le paiement de fonds au nom d'un client;
- Les casinos (sauf certains casinos temporaires à des fins caritatives);
- Les promoteurs immobiliers.

5.2 LA PROTECTION DE LA VIE PRIVÉE ET LA SÉCURITÉ DU PÉRIMÈTRE

Depuis février 2011, les gouvernements canadien et américain travaillent à intégrer leur frontière commune pour accroître la sécurité et faciliter le commerce. Le plan d'action *Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre*, qui a été publié en décembre 2011, contenait des détails relatifs à la mise en œuvre de cette intégration, mais ne prenait pas en considération les recommandations formulées en juin de la même année par le Commissariat.

De plus, aucun des deux gouvernements n'a tenu compte des préoccupations relatives à la protection de la vie privée soulevées par le vaste Plan d'action.

En réaction à cette situation, les commissaires à la protection de la vie privée et les ombudsmans de tout le pays ont émis une résolution conjointe, le 2 avril 2012, alors que le premier ministre Stephen Harper et le président Barack Obama rencontraient à Washington le président du Mexique, Felipe Calderon.

La résolution exhortait le gouvernement fédéral canadien à prendre toutes les mesures nécessaires pour faire en sorte que les normes et les valeurs sous-jacentes aux lois canadiennes en matière de protection de la vie privée ne soient pas abaissées en raison de programmes élaborés aux fins de la mise en œuvre du plan d'action sur la sécurité du périmètre Canada-États-Unis, mieux connu sous le nom de plan d'action *Par-delà la frontière*.

La résolution conjointe énonçait 13 recommandations, dont les suivantes :

- toutes les initiatives découlant du Plan d'action dans le cadre desquelles des renseignements personnels sont recueillis devraient prévoir des mécanismes de recours et de réparation appropriés pour vérifier l'exactitude des fichiers, corriger les erreurs et limiter la communication de l'information à d'autres pays;
- le Parlement, les commissaires à la protection de la vie privée des provinces et la société civile devraient participer à la conception des initiatives du Plan d'action;
- les renseignements sur les Canadiennes et les Canadiens devraient autant que possible être conservés sur le territoire canadien ou du moins être protégés par le Canada;
- les nouvelles technologies de surveillance utilisées au Canada, comme les véhicules aériens sans pilote, doivent être visées par des mesures de contrôle adéquates dans un cadre réglementaire approprié.

Plusieurs préoccupations exprimées dans la résolution ont été abordées dans l'*Énoncé conjoint des principes de protection des renseignements personnels*, que les gouvernements du Canada et des États-Unis ont rendu public le 28 juin 2012. Dans l'annonce officielle toutefois, on pouvait lire ce qui suit : « Cet énoncé des principes de protection de la vie privée ne

vise pas à constituer un traité ou toute autre forme d'accord contraignant en droit international. »

Selon une directive du Conseil du Trésor, tous les programmes du gouvernement fédéral qui nécessitent le traitement de renseignements personnels doivent faire l'objet d'une évaluation des facteurs relatifs à la vie privée, ou EFVP, qui doit ensuite être présentée au Commissariat pour examen. Par conséquent, tous les programmes fédéraux découlant de la mise en œuvre du Plan d'action devront faire l'objet d'un tel examen et seront visés, au besoin, par des recommandations formulées par le Commissariat. Vous trouverez des détails sur les EFVP reçues au cours du dernier exercice en ce qui a trait à la frontière canado-américaine dans la prochaine section du présent chapitre.

Résolution des commissaires canadiens à la protection de la vie privée et des responsables de l'application des lois en matière de protection des renseignements personnels concernant le Plan d'action sur la sécurité du périmètre et la compétitivité économique Canada – États-Unis : http://www.priv.gc.ca/media/nr-c/2012/res_120402_f.asp.

5.3 LE SYSTÈME CANADO-AMÉRICAIN INTÉGRÉ DE CONTRÔLE DES ENTRÉES ET DES SORTIES

Dans le cadre du plan d'action *Par-delà la frontière*, le Canada et les États-Unis mettront systématiquement en commun les renseignements recueillis sur les voyageurs qui traversent leur frontière commune; le fichier d'une personne qui entre dans un pays sera le même que celui où elle quitte le pays.

Le Canada n'a pas, dans le passé, exercé un suivi des sorties des personnes allant aux États-Unis, et l'on s'inquiète du fait que les renseignements recueillis puissent servir à des fins secondaires variées. Pour évaluer sa capacité technique, l'Agence des services frontaliers du Canada (ASFC) a procédé à un essai dans le cadre de la phase 1, qui s'est échelonné d'octobre 2012 à janvier 2013; elle a alors communiqué aux États-Unis les données sur les ressortissants de pays tiers et les ressortissants étrangers qui sont passés à deux postes frontaliers terrestres de l'Ontario et à deux postes frontaliers terrestres de la Colombie-Britannique.

Dans le cadre de la phase II, qui a débuté le 30 juin 2013, le projet a été étendu à tous les postes frontaliers terrestres. Lors des phases à venir, les renseignements concernant tous les voyageurs qui traverseront la frontière à un poste terrestre ou aérien, y compris les citoyens du Canada et des États-Unis, seront communiqués à l'autre pays. Une fois sa mise en œuvre achevée, soit d'ici juin 2014, le programme des entrées et des sorties fournira aux deux pays des données historiques sur la période durant laquelle des Canadiens, des citoyens américains, des résidents permanents, des résidents temporaires et des visiteurs se sont trouvés à l'intérieur et à l'extérieur de leur territoire.

Diverses utilisations secondaires de ces renseignements par des institutions fédérales autres que l'ASFC sont actuellement envisagées.

Nous avons recommandé que des panneaux bien visibles soient installés dans les postes frontaliers pour indiquer la raison pour laquelle les renseignements demandés sont recueillis et les fins auxquelles ils seront utilisés, que le nombre d'utilisations secondaires soit strictement limité et que toute communication de renseignements relatifs aux entrées et aux sorties soit clairement justifiée. Nous nous inquiétons de la longue période de conservation de ces renseignements — 75 ans — et avons demandé à l'ASFC de vérifier s'il existe des raisons suffisantes pour justifier que les renseignements soient conservés pendant une aussi longue période. Nous craignons que des éléments de données supplémentaires comme des empreintes digitales ou des photos s'ajoutent au fur et à mesure de l'évolution du projet. Il y a longtemps que les États-Unis proposent l'instauration d'un système biométrique associé aux sorties pour recueillir les empreintes digitales des visiteurs quittant le pays; un tel système fait l'objet de discussions en Europe.

Nous avons aussi des inquiétudes par rapport à l'échéancier serré qui a été avancé pour la mise en œuvre de ce système et d'autres activités prévues dans le cadre du plan d'action *Par-delà la frontière*. Nous avons reçu l'EFVP de la phase I du programme des entrées et des sorties quelques jours seulement avant le début de l'essai sur le terrain. En réaction à cette question et à d'autres, la commissaire a écrit au président de l'ASFC pour lui faire part de ses préoccupations et demander à ce que les EFVP soient fournies plus tôt dans le processus afin de pouvoir formuler, étudier et mettre en œuvre des recommandations bien avant l'entrée en vigueur d'une initiative.

5.4 ZONES DE CONTRÔLE DES DOUANES

Les zones de contrôle des douanes (ZCD) sont de grandes aires désignées situées à proximité de la frontière ou associées à celle-ci, où les travailleurs et les voyageurs nationaux en partance peuvent entrer en contact avec des marchandises et des voyageurs internationaux qui n'ont pas encore subi le contrôle des services douaniers.

Les nouveaux règlements permettent aux agents de l'ASFC d'arrêter, d'interroger, de détenir, de fouiller et même de procéder à une fouille à nu des personnes qui se trouvent dans ces zones. Les agents peuvent se servir de ces pouvoirs extraordinaires même lorsque les personnes n'ont pas l'intention de traverser la frontière.

Nous avons fait part de notre inquiétude en ce qui a trait au fait que les aires susceptibles d'être désignées comme zones de contrôle des douanes sont étendues et que les voyageurs n'ont aucun moyen de savoir s'ils se trouvent à l'intérieur ou à l'extérieur de celles-ci. Nous avons demandé une signalisation bien visible qui indiquerait les limites de chaque zone et avons recommandé que le bien-fondé de toute désignation

d'une aire en tant que ZCD soit clairement justifié et démontré.

L'ASFC a précisé que des panneaux d'information générale seraient installés aux points d'entrée pour informer les voyageurs qu'il se *pourrait* qu'ils traversent des ZCD, mais que l'emplacement exact de ces zones où des agents des services frontaliers peuvent utiliser leurs pouvoirs extraordinaires ne serait pas indiqué.

5.5 TRAITÉ SUR L'ÉCHANGE DE RENSEIGNEMENTS EN MATIÈRE D'IMMIGRATION

Depuis de nombreuses années, Citoyenneté et Immigration Canada (CIC) et le Département d'État des États-Unis échangent des renseignements au cas par cas lorsque des soupçons justifient la collecte de données additionnelles afin de pouvoir prendre des décisions au sujet de demandeurs de visa ou de demandeurs du statut de réfugié.

Le plan d'action *Par-delà la frontière* élargit considérablement cet échange. Chaque pays interrogera systématiquement et automatiquement les systèmes de données sur l'immigration de l'autre pays pour obtenir des renseignements négatifs ou à caractère dérogatoire sur tous les demandeurs de visa de pays tiers.

Les renseignements recueillis au moyen de ces recherches serviront à déterminer l'admissibilité.

Nous craignons que cette initiative n'augmente considérablement la quantité de renseignements à caractère dérogatoire recueillis par CIC et que certains de ces renseignements ne soient pas nécessaires ou ne s'appliquent pas aux lois canadiennes sur l'immigration.

Nous avons recommandé que CIC définisse clairement le type de renseignement qui sera considéré comme étant « à caractère dérogatoire » afin que seuls des renseignements exacts et pertinents servent à la prise de décisions dans le domaine de l'immigration. Nous avons reçu et examiné une EFVP concernant l'aspect relatif à l'échange de renseignements biographiques dans le cadre de ce programme en 2013, et nous prévoyons recevoir une autre EFVP sur l'échange d'empreintes digitales et de photos en 2014.

5.6 PROJET DE BIOMÉTRIE POUR LES RÉSIDENTS TEMPORAIRES

Le Projet de biométrie pour les résidents temporaires est un projet interministériel géré conjointement par CIC, l'ASFC et la Gendarmerie royale du Canada (GRC). Il vise à saisir, à associer et à vérifier des renseignements biométriques de ressortissants étrangers qui présentent une demande pour entrer au Canada à titre de visiteur, d'étudiant ou de travailleur. À partir de la fin de 2013, les ressortissants étrangers de certains pays qui souhaitent obtenir un visa pour entrer au Canada devront fournir leurs empreintes

digitales et se faire photographier dans le cadre de leur demande.

Nous avons consulté les trois organismes au sujet de l'évolution du projet et avons reçu deux nouvelles EFVP au Commissariat en 2012-2013. Un changement important a été apporté depuis que nous avons examiné l'EFVP transitoire : la GRC aura l'autorisation de conserver les renseignements, y compris les empreintes digitales prises pendant le processus de demande de visa, et d'utiliser ces données à des fins d'application des lois au pays. Les empreintes digitales de personnes présentant une demande de visa pour entrer au Canada à titre de visiteur, de travailleur ou d'étudiant seront conservées par la GRC pendant au moins 15 ans; les empreintes digitales prises par la police dans le cadre d'enquêtes criminelles, y compris les empreintes latentes prélevées sur des scènes de crime, peuvent maintenant être comparées aux empreintes conservées dans cette base de données. Nous sommes préoccupés par la longue période de conservation ainsi que par les utilisations possibles des empreintes digitales de personnes qui n'ont pas été accusées ou déclarées coupables d'une infraction criminelle.

Comme c'est le cas avec de nombreux programmes relevant du plan d'action *Par-delà la frontière*, nous avons des inquiétudes au sujet des échanges courants à grande échelle de renseignements avec d'autres pays, puisqu'une fois que les renseignements ont traversé la frontière du Canada, il peut être difficile, voire impossible, de prévenir l'utilisation, la communication ou le transfert non autorisés de ces renseignements, ou de garantir qu'ils seront bien protégés.

5.7 CENTRES DE RÉCEPTION DES DEMANDES DE VISA À L'ÉTRANGER

Les centres de réception des demandes de visa exploités à l'étranger par des fournisseurs de services du secteur privé sous contrat avec CIC constituent un autre élément du Projet de biométrie pour les résidents temporaires (PBRT). Ces centres offrent des services aux étudiants, aux travailleurs et aux visiteurs à destination du Canada qui ont besoin d'un visa de résident temporaire et ils recueilleront aussi des renseignements liés à la présentation d'une demande, y compris des empreintes digitales et des photos, comme l'exige le PBRT. Les demandes dûment remplies seront transférées électroniquement à CIC, et les empreintes digitales seront conservées par la GRC dans une base de données faisant partie de son Système d'identification en temps réel.

Nous avons formulé un certain nombre de recommandations liées aux mesures de protection des renseignements biométriques confidentiels et à l'importance d'en assurer l'exactitude. Nous avons également exprimé des préoccupations concernant les risques d'atteinte à la vie privée découlant de mesures législatives divergentes possibles dans la localité où se trouve un centre.

Nous avons recommandé que CIC procède à un examen des administrations locales avant d'octroyer des contrats pour évaluer les mesures de protection de la vie privée et les risques d'atteinte. Nous prévoyons recevoir, à l'automne 2013, une EFVP liée à la dernière phase du projet des centres de réception des demandes de visa.

5.8 FAITS NOUVEAUX SUR L'ACCÈS LÉGAL

Depuis le milieu des années 1990, le Commissariat examine périodiquement différentes propositions du gouvernement fédéral visant à redéfinir le cadre juridique du Canada qui régit l'utilisation de la surveillance électronique.

En février 2012, le gouvernement a présenté le projet de loi C-30, la plus récente version d'une loi sur l'accès dit « légal ». Comme plusieurs projets de loi depuis 2005, cette mesure législative proposait de donner à l'État des moyens juridiques accrus de surveillance et d'accès aux renseignements personnels.

La loi (aussi appelée *Loi sur la protection des enfants contre les cyberprédateurs*) aurait accordé aux autorités les nouveaux pouvoirs suivants :

- assurer la surveillance et le suivi des activités numériques de la population canadienne en temps réel;
- exiger des fournisseurs de services qu'ils conservent les métadonnées, le contenu et les communications de leurs abonnés, et les communiquent sur réception d'une ordonnance de communication;
- obliger les fournisseurs de services à fournir des renseignements sur les abonnés sans devoir présenter un mandat ou sans faire l'objet d'un contrôle judiciaire;
- une capacité d'interception obligatoire à l'égard de tous les dispositifs et services, permettant ainsi un accès à distance secret aux fichiers et aux communications électroniques des personnes.

Le Commissariat a déclaré à maintes reprises qu'il comprenait les défis auxquels font face les organismes chargés de la sécurité nationale et de l'application de la loi dans la lutte contre la cybercriminalité, particulièrement dans le contexte actuel de la révolution des technologies des communications.

L'adoption de toute loi ayant pour effet d'élargir les modalités d'une surveillance électronique par l'État devrait toutefois être appuyée par des arguments démontrant qu'elle protège le public, respecte les principes fondamentaux de protection de la vie privée établis dans le droit canadien et est assujettie à la surveillance appropriée.

Peu de temps après le dépôt du projet de loi C-30, le Commissariat a cerné d'importants enjeux liés à la protection de la vie privée, semblables à ceux qu'il a cernés en ce qui a trait aux projets de loi antérieurs sur l'accès légal. Nous nous préoccupions en particulier de l'accès, sans mandat, aux

renseignements sur les abonnés. Ainsi, permettre aux autorités d'exiger des noms, des adresses domiciliaires, des détails sur des comptes de courrier électronique et des adresses IP pour des raisons liées au maintien de l'ordre, sans surveillance judiciaire, nous semblait un élargissement considérable des pouvoirs. Un simple exemple : une adresse IP peut s'apparenter à une empreinte digitale et constituer un point de départ à partir duquel il est possible de dresser un tableau des activités en ligne d'une personne, y compris son abonnement à des services en ligne, ses intérêts personnels selon les sites Web consultés, ses affiliations professionnelles et même son emplacement physique.

Comme ce vaste pouvoir n'était pas limité aux cas pour lesquels il existait des motifs raisonnables de soupçonner des activités criminelles ou aux enquêtes criminelles, le projet de loi risquait d'avoir des répercussions sur les citoyens respectueux des lois.

De nombreux Canadiens ont réagi fortement contre le projet de loi, soutenant qu'il aurait une incidence négative de taille sur leur droit fondamental à la vie privée.

CE QU'UNE ADRESSE IP PEUT RÉVÉLER À VOTRE SUJET

« C'est la même chose que de consulter l'annuaire téléphonique pour connaître les coordonnées d'une personne. » Voilà l'argument avancé par les défenseurs de mesures législatives sur « l'accès légal », comme le projet de loi C-30, qui laisserait les organismes responsables de l'application de la loi et de la sécurité nationale recueillir des renseignements sur les abonnés d'Internet sans obtenir au préalable l'autorisation d'un juge.

Dans le même ordre d'idées, la collecte sans mandat des métadonnées qui font partie de toutes les communications par Internet a été comparée à la lecture de ce qui serait écrit sur une enveloppe.

Le Commissariat a procédé à des essais techniques approfondis afin d'examiner les répercussions sur la protection de la vie privée de la collecte éventuelle, en vertu du projet de loi C-30, de renseignements sur les abonnés d'Internet, collecte qui ne se limite pas aux renseignements figurant dans un annuaire téléphonique comme le nom, l'adresse et le numéro de téléphone.

Ces renseignements additionnels sur les abonnés englobaient les adresses électroniques, les numéros de téléphone cellulaire et les adresses individuelles de protocole Internet (IP), qui sont attribuées par les fournisseurs de services à tous les dispositifs électroniques des abonnés qui utilisent leur réseau. Chaque version d'un projet de loi sur l'accès légal au Canada déposée au cours des dernières années (comme le précédent projet de loi C-52) aurait obligé les fournisseurs de services Internet à fournir sur demande ces renseignements aux autorités.

En général, les résultats de notre étude nous ont permis de conclure que, contrairement aux simples données contenues dans un annuaire téléphonique, les adresses électroniques, les numéros de téléphone mobile et les adresses IP peuvent servir à dresser un profil très détaillé d'une personne révélant ainsi ses activités, ses opinions, ses intérêts, ses penchants et son style de vie.

L'étude intégrale peut être consultée sur notre site Web, à l'adresse suivante : http://www.priv.gc.ca/information/research-recherche/2013/ip_201305_f.pdf.

Le 11 février 2013 — presque exactement un an après le dépôt du projet de loi C-30 —, le ministre de la Justice, Rob Nicholson, a annoncé que le gouvernement n'irait pas de l'avant avec ce texte législatif. Il a aussi déclaré que toute proposition future visant à moderniser le *Code criminel* ne contiendrait pas les mesures prévues dans le projet de loi C-30, y compris la communication obligatoire, sans mandat, de renseignements de base sur les abonnés, ou l'exigence, pour les entreprises de services de télécommunications, d'intégrer une capacité d'interception à leurs systèmes.

Dans une déclaration, la commissaire Stoddart a salué l'annonce du gouvernement comme « une bonne nouvelle pour la protection de la vie privée au Canada ».

« Je tiens à féliciter l'ensemble des Canadiennes et des Canadiens qui ont exprimé leurs préoccupations par rapport au projet de loi et leur grand attachement à l'égard de leur droit à la vie privée », a ajouté la commissaire.

5.9 L'ÉCOUTE ÉLECTRONIQUE EN CAS D'URGENCE — LE PROJET DE LOI C-55

En avril 2012, la Cour suprême du Canada a déclaré inconstitutionnel un article du *Code criminel* qui donnait accès, sans autorisation judiciaire préalable, aux communications privées dans une situation d'urgence. L'affaire *R. c. Tse* découle d'un présumé enlèvement survenu en Colombie-Britannique pendant lequel des policiers ont procédé à l'interception de communications privées sans autorisation judiciaire, en invoquant le caractère urgent de la situation.

La Cour a jugé inconstitutionnels certains aspects de la loi et a donné au gouvernement jusqu'au 13 avril 2013 pour rendre la loi compatible avec la *Charte* :

- en précisant que seuls les policiers — et non tous les agents de la paix —peuvent faire de l'écoute électronique, et ce, uniquement dans le cas de crimes graves;
- en veillant à ce que les personnes dont les communications privées ont été interceptées en raison d'une situation d'urgence en soient informées dans un délai de 90 jours;
- en ordonnant que le public soit informé de toutes les interceptions effectuées dans des situations d'urgence.

Le gouvernement fédéral a répondu en accélérant le processus relatif au projet de loi C-55, notamment par la tenue, le 25 mars 2013, d'une audience du Comité sénatorial permanent des Affaires juridiques et constitutionnelles. Dans son témoignage devant le Comité, la commissaire adjointe Chantal Bernier a décrit le projet de loi C-55 comme un pas dans la bonne direction en matière de protection de la vie privée.

La commissaire adjointe a aussi indiqué que le pouvoir de surveiller les communications privées des

Canadiennes et des Canadiens était l'un des pouvoirs les plus intrusifs jamais accordé aux enquêteurs. En 2010, le Commissariat avait cerné les principaux points à prendre en considération lors d'interceptions, comme la justification empirique de leur nécessité, ainsi que la responsabilité et la transparence.

La commissaire adjointe a ajouté que l'approche adoptée pour le projet de loi C-55 s'inscrivait exactement dans le cadre d'une analyse mise au point par le Commissariat puisqu'elle limitait la violation de la vie privée aux éléments absolument nécessaires à la sécurité.

Le projet de loi C-55 a été adopté seulement deux jours après l'audience du Comité et a reçu la sanction royale le 27 mars 2013.

5.10 L'UTILISATION DE VÉHICULES AÉRIENS SANS PILOTE PAR LE GOUVERNEMENT FÉDÉRAL

Les reportages diffusés par les médias et l'accroissement de l'activité de délivrance de permis ont incité le Commissariat, à l'automne 2012, à demander à certaines institutions fédérales de l'information sur leur utilisation actuelle et prévue des véhicules aériens sans pilote (UAV). Au Canada, les UAV sont considérés comme des aéronefs aux termes de la *Loi sur l'aéronautique* et doivent donc être utilisés en respectant les limites prescrites par Transports Canada dans le *Règlement de l'aviation canadien*.

Nous avons communiqué avec un certain nombre d'institutions qui, selon nous, étaient susceptibles d'utiliser des UAV, dont la Gendarmerie royale du Canada (GRC) et le ministère de la Défense nationale (MDN), mais quelques-unes seulement nous ont répondu. Au moment de rédiger le présent rapport, nous avions notamment reçu une réponse de la part de la GRC, qui nous a expliqué qu'elle utilisait cette technologie pour obtenir de l'information sur des scènes d'accidents de voiture et pour effectuer des activités de recherche et de sauvetage. Elle a soutenu qu'elle n'utilisait pas les UAV pour surveiller ou recueillir des renseignements personnels. De son côté, le MDN a indiqué qu'il utilisait les UAV, mais uniquement dans le cadre d'opérations sur le terrain à l'extérieur du Canada. Le Conseil national

En octobre et en novembre 2012, le Commissariat a commandé un sondage auprès de 1 531 Canadiennes et Canadiens sur les enjeux liés à la protection de la vie privée, dont leurs perceptions à l'égard de l'utilisation des véhicules UAV. Si quatre répondants sur cinq ont déclaré être très à l'aise avec l'utilisation des UAV par les autorités d'application de la loi dans le cadre de missions de recherche et de sauvetage, leur nombre est passé à deux sur cinq quand il s'agit de les utiliser pour surveiller une manifestation ou un événement public.

Le rapport intégral peut être consulté à l'adresse suivante : http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_f.asp.

de recherches du Canada prévoyait en faire une utilisation très limitée pour des essais visant à améliorer la navigation.

Compte tenu de la capacité des UAV de fonctionner en secret, du risque qu'ils soient utilisés à des fins de surveillance générale et de leur importance croissante — y compris dans le domaine civil —, le Commissariat surveillera de près leur utilisation élargie. Nous avons réalisé une recherche approfondie sur les incidences des UAV sur la protection de la vie privée, qui continueront de se préciser à mesure que nous en saurons davantage sur le déploiement de cette technologie.

Nous continuerons aussi à collaborer avec les institutions fédérales de façon à ce que toute utilisation planifiée des UAV se fasse conformément aux exigences en matière de protection de la vie privée. Nous encourageons fortement les institutions qui envisagent d'utiliser les UAV à effectuer en premier lieu une évaluation des facteurs relatifs à la vie privée afin de bien connaître les risques possibles d'atteinte à la vie privée et de déterminer des mesures d'atténuation.

5.11 RENSEIGNEMENTS SUR LES VOYAGEURS AÉRIENS — PROJET DE LOI C-45

Le Commissariat a fait des présentations devant deux comités parlementaires au sujet d'un changement, petit mais toutefois significatif, à un programme qui a déjà d'importantes répercussions sur les voyageurs aériens.

Ce programme porte sur la collecte, l'utilisation et la communication de renseignements personnels potentiellement sensibles sur les personnes arrivant au Canada par voie aérienne. Il comporte deux volets interreliés : le volet Information préalable sur les voyageurs (IPV) et le volet Dossier passager (DP).

Les renseignements recueillis dans le cadre du volet IPV sont les renseignements « biographiques » qui figurent dans le passeport ou dans les documents de voyage; ils ne changent donc pas beaucoup. Quant aux renseignements recueillis dans le cadre du volet DP, ils changent d'un voyage à l'autre, car ils sont composés des renseignements qui figurent habituellement dans un système de réservations automatisé, comme l'itinéraire du voyage, la méthode de paiement du billet, le nombre de bagages enregistrés et le numéro du siège.

Les renseignements recueillis dans le cadre du volet DP peuvent être beaucoup plus révélateurs car ils peuvent fournir des renseignements sensibles sur les compagnons de voyage et sur la personne qui a acheté le billet. Ces renseignements peuvent notamment indiquer si la personne a commandé un repas spécial ce qui permettrait de faire des inférences sur la religion, l'ethnicité ou l'état de santé du voyageur. Les autorités frontalières peuvent se servir des renseignements recueillis dans le cadre du volet DP pour créer des profils des voyageurs et tirer des conclusions à leur sujet.

La modification, en apparence mineure, qui est incluse à titre d'article dans l'important projet de loi omnibus sur le budget (projet de loi C-45) oblige les transporteurs aériens à fournir les renseignements

correspondant au volet IPV et au volet DP à l'Agence des services frontaliers du Canada (ASFC) et cela, non seulement au sujet des personnes à bord, mais aussi de celles qui sont censées être à bord.

Dans un mémoire présenté au Comité permanent de la sécurité publique et nationale de la Chambre des communes, la commissaire Stoddart a écrit que les transporteurs aériens seraient désormais obligés de fournir des renseignements à l'ASFC encore plus tôt qu'ils ne le font actuellement, y compris des renseignements sur les personnes qui ont annulé leur voyage à la dernière minute.

« Nous croyons comprendre que les changements proposés découlent du *Plan d'action sur la sécurité du périmètre et la compétitivité économique* Canada-États-Unis et, possiblement, des négociations continues entre le Canada et la Commission européenne pour l'obtention d'un nouvel accord sur le volet DP. En règle générale, la nouvelle approche relative à la prise de décisions lors du contrôle des passagers consiste à utiliser l'information préalable sur les voyageurs pour approuver ou refuser l'embarquement sur les vols à l'étranger », a ajouté la commissaire.

Le Commissariat a souvent exprimé des préoccupations à propos du manque de transparence concernant l'utilisation qui est faite des renseignements recueillis sur les passagers dans le cadre des volets IPV/DP. De plus, de nombreux détails du programme sont négociés en secret avec d'autres pays.

Le Commissariat a régulièrement relevé des problèmes liés au fait que les renseignements personnels recueillis par les volets IPV/DP du programme de l'ASFC sont communiqués, à grande échelle, à d'autres organismes fédéraux (comme la GRC et le Service canadien du renseignement de sécurité), à des homologues des provinces et à des partenaires d'autres administrations.

La commissaire adjointe Chantal Bernier a exprimé une bonne partie des mêmes préoccupations dans son témoignage devant le Comité sénatorial permanent des transports et des communications.

Elle a aussi indiqué que les volets IPV/DP devraient être examinés en lien avec les autres programmes du genre, comme le Programme de protection des passagers (PPP ou liste des personnes interdites de vol) ainsi que le nouveau programme d'Autorisation de voyage électronique (AVE), aussi proposé dans le projet de loi C-45. L'AVE obligera les ressortissants des pays visés par une mesure de dispense de visa, soit de la plupart des pays européens, à présenter un formulaire de demande à Citoyenneté et Immigration Canada avant de venir au Canada.

« Les liens entre les volets IPV/DP et le programme d'Autorisation de voyage électronique proposé et le PPP nous semblent peu clairs et, si tel est le cas pour nous, nous doutons que la population canadienne comprenne la manière dont les programmes sont liés entre eux », a déclaré la commissaire adjointe.

Le projet de loi C-45 a été approuvé sans modification par le Parlement et a été adopté le 14 décembre 2012.

6.0 Le Commissariat à l'œuvre

Au moment où la *Loi sur la protection des renseignements personnels* amorce sa quatrième décennie — elle approche de l'âge moyen selon les normes humaines — la mission du Commissariat consiste toujours à protéger et à préserver le droit à la vie privée des personnes dans leurs rapports avec les 250 institutions et organismes fédéraux régis par la *Loi*.

Toutefois, cette mission est devenue beaucoup plus complexe et difficile, car les institutions fédérales continuent d'accroître leurs inventaires de renseignements personnels sur les Canadiens de même que leur capacité technologique de traiter ces données.

Ce chapitre présente un aperçu de la façon dont le Commissariat a su relever ce défi au cours du dernier exercice. Il fournit un aperçu détaillé des mesures que nous avons prises en ce qui a trait aux enquêtes, devant le Parlement, devant les tribunaux et quant au suivi des vérifications précédentes afin de voir comment nos recommandations ont été mises en œuvre par les institutions pour ce qui est de l'élimination des renseignements et de l'utilisation d'appareils sans fil.

En outre, le chapitre donne des explications sur l'augmentation considérable du nombre de plaintes reçues au cours de la dernière année, en plus de donner une idée des préoccupations communiquées par les citoyens à notre Centre d'information. De plus, il présente des exemples de réussite clés dans le cadre desquels des institutions ont profité de l'occasion qui leur était offerte de répondre aux besoins du plaignant au moyen du processus de règlement rapide, plutôt que de recourir à la procédure impliquant une enquête plus officielle et, parfois, très longue.

6.1 ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Depuis 2002, le Secrétariat du Conseil du Trésor du Canada (SCT) demande aux ministères et aux organismes fédéraux de réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) dès les premières étapes de l'élaboration d'initiatives qui comportent des risques liés à la vie privée, et de la

présenter au Commissariat aux fins d'examen. On vise ainsi à déterminer les risques d'atteinte à la vie privée et à élaborer des stratégies pour les éliminer ou les atténuer.

Le Commissariat demande que, dans le cadre de ce processus, les institutions fédérales se posent les quatre questions suivantes : L'initiative est-elle absolument nécessaire? Permettra-t-elle vraisemblablement d'atteindre les objectifs visés? La perte de confidentialité qui résultera de l'initiative est-elle proportionnelle aux avantages attendus? Existe-t-il d'autres façons de faire moins envahissantes pour la vie privée?

Une fois que les institutions fédérales ont répondu à ces questions, nous leur demandons de démontrer que la collecte est appropriée et limitée aux renseignements absolument nécessaires, que les renseignements recueillis seront protégés adéquatement, que l'utilisation et la communication des renseignements se font de façon appropriée et sont assujetties à des mesures de contrôle, et que les renseignements seront éliminés conformément à la *Loi sur la protection des renseignements personnels*.

Bien que nous ayons toujours prodigué des conseils aux institutions à diverses étapes du processus d'EFVP, nous avons décidé, en 2012-2013, d'étendre nos activités de consultation informelles. Ces consultations informelles nous permettent de donner des conseils plus tôt au cours du processus, et d'être informés des initiatives avant la réception d'une EFVP. Notre processus d'examen est davantage ciblé, de façon à ce que nos ressources soient consacrées aux initiatives qui posent les risques les plus élevés en matière de protection des renseignements personnels et que nos conseils soient offerts en temps opportun afin de garantir leur pertinence et de permettre aux institutions de mettre en œuvre nos recommandations le plus rapidement possible.

Nous n'approuvons pas les évaluations ni ne souscrivons à des projets ou à des propositions au cours de notre examen. Nous ne pouvons pas non plus obliger les institutions à mettre en œuvre nos recommandations, ni même à tenir compte de nos conseils. Cela dit, nous constatons que les ministères et organismes sont généralement prêts à travailler avec nous pour régler les préoccupations liées à la vie privée.

Les Canadiens bénéficient également de la transparence conférée par le processus d'EFVP lorsque les ministères et organismes publient sur leur site Web des résumés des évaluations réalisées.

En 2012-2013, nous avons reçu 68 nouvelles EFVP et tenu 22 consultations tout en poursuivant notre travail sur les dossiers d'initiatives soumises antérieurement. Nous avons envoyé 20 lettres de recommandations détaillées et exhaustives au sujet d'initiatives que nous avons jugées particulièrement envahissantes, en plus d'envoyer 29 autres lettres contenant des recommandations moins détaillées au sujet d'initiatives qui, à notre avis, comportaient des risques plus faibles.

Voici les points saillants de certaines évaluations dignes de mention.

6.1.1 Agence des services frontaliers du Canada — Norme relative aux enquêtes de sécurité sur le personnel

Le Commissariat a reçu une EFVP pour le programme remanié d'enquêtes de sécurité de l'Agence des services frontaliers du Canada (ASFC), la Norme d'intégrité élevée pour les enquêtes de sécurité sur le personnel, peu de temps avant sa mise en œuvre en juin 2012. En raison du moment où l'EFVP a été soumise, nous n'avons pu l'examiner avant que le programme d'enquêtes de sécurité devienne opérationnel.

En l'espace de quelques jours, le programme faisait les manchettes, principalement en raison d'un questionnaire sur l'intégrité qui demandait aux employés de l'Agence — et aux employés potentiels — s'ils avaient déjà consommé des drogues ou de l'alcool, joué à des jeux de hasard, eu recours aux services de prostituées, fait du tourisme sexuel ou téléchargé des images de bestialité.

Nous avons cerné des risques importants d'atteinte à la vie privée lors de notre examen de la norme relative aux enquêtes de sécurité, plus particulièrement pour ce qui est des questions générales très indiscrètes. Le Commissariat a formulé des recommandations à l'intention de l'Agence quant au caractère envahissant du questionnaire, et il a également fait part de ses préoccupations concernant le consentement, l'avis et les mesures de sécurité.

Nous nous préoccupions par ailleurs de l'application trop générale de l'ensemble du programme aux employés dont les tâches ne nécessitaient pas l'accès à des renseignements et à des biens sensibles, ainsi que par le manque de preuves à l'appui de la nécessité et de l'efficacité de la norme relative aux enquêtes de sécurité.

Pour donner suite à nos recommandations, l'ASFC a cessé d'utiliser le questionnaire en octobre 2012. Elle l'a révisé depuis afin de supprimer ou de modifier des questions peu susceptibles de faire la preuve de la loyauté et de la fiabilité d'une personne. Néanmoins, le Commissariat continue d'avoir de graves préoccupations quant à l'absence de preuves pour justifier la nécessité d'avoir recours à la norme relative aux enquêtes de sécurité en plus du service fourni pour le compte du gouvernement fédéral par le Service canadien du renseignement de sécurité (SCRS), ou pour appuyer l'efficacité de ces questionnaires en vue de l'atteinte des objectifs visés.

6.1.2 Surveillance audio aux points d'entrée

Le Commissariat discute avec l'ASFC de l'utilisation de la surveillance vidéo avec support audio aux points d'entrée depuis la présentation d'une EFVP à ce sujet en 2011.

Notre examen de l'EFVP avait suscité de vives inquiétudes quant à l'utilisation intensive de l'audio et de la vidéo pour enregistrer les voyageurs aux points d'entrée; à l'époque, l'Agence nous avait indiqué que le projet avait été annulé.

Nous avons de nouveau communiqué avec l'Agence relativement à cette question à la suite de la diffusion,

en juin 2012, de reportages par les médias faisant état de la mise en place de mesures en vue de la surveillance audio-vidéo dans certains aéroports canadiens. Suite à la tenue de plusieurs réunions de consultation et à l'envoi de lettres faisant état de nos préoccupations, l'Agence nous a assurés que les activités d'enregistrement audio avaient été suspendues aux points d'entrée, dans l'attente de la présentation d'une nouvelle EFVP. Il importe de signaler que les salles d'entrevue de l'Agence, où les voyageurs soupçonnés d'infractions douanières sont interrogés, ne sont pas visées par cette décision. Au moment de la rédaction du présent rapport, nous n'avions pas encore reçu de nouvelle EFVP.

6.1.3 Secrétariat du Conseil du Trésor du Canada — Norme sur la protection de la vie privée et l'Analytique Web

L'analytique Web est la collecte et l'analyse de données sur le trafic Web et les visites d'utilisateurs dans le but de comprendre et d'optimiser l'utilisation du Web. En règle générale, les outils d'analytique Web enregistrent l'interaction des visiteurs avec les pages Web en recueillant les adresses du protocole Internet (adresses IP) de ces visiteurs.

Le Commissariat examine l'utilisation de l'analytique Web par les institutions gouvernementales depuis 2010. En juin 2011, nous avons exprimé nos préoccupations par rapport à l'absence de directives officielles du Secrétariat du Conseil du Trésor du Canada (SCT) visant à favoriser une utilisation de l'analytique Web par les institutions qui tienne compte de la protection de la vie privée. Pour donner suite à nos préoccupations, le SCT a rédigé la nouvelle Norme sur la protection de la vie privée et le Web analytique et réalisé une EFVP sur les risques connexes.

Après de longues discussions entre le Commissariat et le SCT, des versions définitives de l'EFVP et de la Norme prévoyant des échéanciers pour la conservation et l'élimination des renseignements personnels recueillis dans le cadre de l'analytique Web ont été approuvées. Le profilage de l'utilisation Web des personnes au moyen de l'analytique est expressément interdit. La Norme comporte également une liste détaillée d'exigences relatives aux avis de confidentialité en ce qui concerne l'analytique Web.

Même si nous sommes heureux de constater que des mesures ont été mises en œuvre en réponse à la plupart de nos recommandations, nous continuons de préconiser que le SCT fournisse aux institutions des directives concrètes pour la réalisation d'EFVP portant sur l'utilisation du Web analytique.

6.1.4 Services partagés Canada — Authentification par CléGC

Comme l'indique notre rapport annuel 2011-2012, nous continuons de suivre l'évolution de la stratégie de renouvellement de l'authentification électronique. Jusqu'à la fin de 2012, Services partagés Canada (SPC) supervisait un service de clé d'accès qui authentifiait les entreprises et les personnes dans le cadre de leurs interactions en ligne avec le gouvernement du Canada.

Nous avons examiné la CléGC, le service d'authentification exclusif au GC qui a remplacé la Clé d'accès. La CléGC permet aux entreprises et aux personnes d'ouvrir une session dans les programmes et les services du gouvernement fédéral à l'aide d'une combinaison formée d'un nom d'utilisateur et d'un mot de passe de leur choix.

Le Commissariat était préoccupé par l'absence d'un calendrier de conservation et de retrait des renseignements personnels dans la CléGC. En outre, le processus de création du mot de passe n'incluait pas un test pour s'assurer que les mots de passe choisis ne contiennent pas de mots courants du dictionnaire. Nous avons recommandé que SPC établisse un calendrier de conservation et de retrait des données comportant des renseignements personnels, comme les fichiers journaux produits par la CléGC et les questions et réponses liées aux justificatifs d'identité de celle-ci.

Nous avons également recommandé d'ajouter un test du dictionnaire lors du processus de création du mot de passe afin d'accroître la sécurité des mots de passe individuels et la sécurité globale du service d'authentification de la CléGC. En bref, ce test fait en sorte qu'une personne ne puisse pas choisir comme mot de passe un mot qu'on peut trouver dans un dictionnaire et qui, par conséquent, est susceptible d'être deviné ou déchiffré par un logiciel ayant recours à la technique d'« attaque par dictionnaire ».

SPC a examiné l'architecture globale de la CléGC, mais il ne s'est pas penché sur la façon dont les ministères procéderaient à la mise en œuvre de ce service. Nous nous attendons à ce que les ministères fédéraux effectuent leurs propres évaluations des risques, ce qui comprend la réalisation d'une EFVP et la présentation de celle-ci au Commissariat, avant d'adopter la CléGC.

Nous avons déjà examiné une EFVP de Ressources humaines et Développement des compétences Canada (maintenant appelé Emploi et Développement social Canada) portant sur l'adoption de la CléGC, et nous nous attendons à recevoir davantage d'EFVP de la part d'autres institutions s'apprêtant à passer de la Clé d'accès à la CléGC.

6.1.5 Citoyenneté et Immigration Canada — Système mondial de gestion des cas

En 2000, Citoyenneté et Immigration Canada a procédé à la mise en œuvre du Système mondial de gestion des cas (SMGC), qui avait été conçu pour remplacer des systèmes plus anciens et permettre une gestion intégrée des cas en matière d'immigration. De nouvelles fonctions correspondant à d'autres secteurs d'activité du Ministère seront intégrées au nouveau système, destiné à remplacer l'important Système de soutien des opérations des bureaux locaux (SSOBL), qui est actuellement utilisé par un grand nombre d'institutions dans l'exécution du travail de contrôle et d'application de la loi dans le secteur de l'immigration.

Le Commissariat a examiné la première version du SMGC en 2004, et la deuxième, cette année. Nous avons cerné plusieurs risques liés à la vie privée concernant la protection des données sensibles, et

avons formulé des recommandations à cet égard. En outre, nous avons constaté que l'EFVP ne donnait pas un aperçu exhaustif de la circulation des renseignements personnels à l'intérieur et à l'extérieur du nouveau système.

À la lumière du rôle clé du SMGC dans la prestation de nombreux programmes et initiatives en matière d'immigration, nous avons entrepris un projet d'une durée de deux mois afin de recenser tous les transferts électroniques de données à destination et en provenance de ce système. Cela nous a permis de mieux comprendre dans quelle mesure les données contenues dans ce système sont consultées et mises en commun avec d'autres institutions, tant au niveau provincial que fédéral. Nous avons répertorié plus de 30 systèmes et interfaces directement liés au SMGC qui reçoivent des données de ce système ou lui transmettent de l'information, ou encore qui remplissent ces deux fonctions.

De plus, nous avons organisé une visite sur place pour observer directement la façon dont les données sont consultées et utilisées par les utilisateurs du SMGC, et pour voir une démonstration des interactions du système avec d'autres systèmes et interfaces réseautés. Cette visite a grandement enrichi notre connaissance du SMGC et nous a aidés dans notre évaluation des risques potentiels d'atteinte à la vie privée du système. Nous continuerons de suivre de près ce dossier au fil de l'évolution du SMGC.

6.1.6 Suivi — Administration canadienne de la sûreté du transport aérien et scanners corporels

Après des années de consultation avec le Commissariat au sujet des scanners corporels, l'Administration canadienne de la sûreté du transport aérien (ACSTA) nous a informés cette année qu'elle mettrait en œuvre la technologie de reconnaissance automatisée des menaces dans des aéroports partout au Canada. Ce logiciel permet le transfert direct de toutes les anomalies détectées par les scanners sous forme de représentation schématique — qui est la seule image que l'agent de contrôle peut voir. Cette méthode élimine le visionnement d'une image réelle du voyageur et fait suite à une recommandation clé du Commissariat préconisant que l'ACSTA explore les technologies d'amélioration de la protection de la vie privée pour les scanners corporels.

6.1.7 Favoriser la conformité — Affichage indiquant une surveillance vidéo sur la Colline du Parlement

La Gendarmerie royale du Canada (GRC) étend sa couverture de la surveillance vidéo sur la Colline du Parlement en installant 134 caméras vidéo de plus que les 50 actuellement en place. Certaines des nouvelles caméras prennent des vues panoramiques et sont dotées d'une fonction zoom. Comme l'indique notre rapport annuel de 2011-2012, nous étions préoccupés par le fait que les visiteurs de la Colline du Parlement ne soient pas informés de

la surveillance vidéo par des affiches, et que cela puisse porter atteinte à leur droit à la vie privée, plus particulièrement lors de manifestations pacifiques.

Nous avons recommandé que des affiches informant les visiteurs qu'ils sont filmés et indiquant le nom d'une personne-ressource à consulter pour obtenir de plus amples renseignements soient installées bien en vue à proximité des entrées de la Colline du Parlement. La GRC, qui travaille en partenariat avec Travaux publics et Services gouvernementaux Canada, la Chambre des communes, le Sénat, la Commission de la capitale nationale, Parcs Canada et d'autres organisations dans le cadre de ce projet, nous a invités à transmettre ce message aux responsables de l'affichage sur la Colline du Parlement et a fourni à ses partenaires de projet notre publication, *Lignes directrices du CPVP concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics* .

Nous continuons de collaborer avec les responsables de l'affichage au moment où ils travaillent à l'installation finale des affiches sur la Colline du Parlement et aux alentours.

Lignes directrices du CPVP concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics..
www.priv.gc.ca/sureveillanceorientation

6.2 ENQUÊTES RÉALISÉES

Outre les enquêtes liées aux technologies de l'information et à l'accès inapproprié que nous avons présentées plus haut, nous avons réalisé, au cours de l'année, de nombreuses autres enquêtes dignes d'intérêt. En voici quelques-unes.

6.2.1 Le refus comme point de départ pour le Service correctionnel du Canada

Entre septembre et décembre 2010, un détenu d'un établissement correctionnel à sécurité maximale a demandé 18 enregistrements vidéo d'incidents dans lesquels il a été impliqué, et qui montrent, selon ce qu'il allègue, des agents du Service correctionnel du Canada (SCC) commettant des voies de fait, des crimes haineux et du harcèlement sexuel.

Le SCC a refusé de fournir les vidéos, en affirmant que celles-ci comprenaient des renseignements personnels de tiers qui ne pouvaient pas être raisonnablement dissimulés, et que la communication de l'information serait préjudiciable à la sécurité d'un établissement correctionnel.

Le plaignant alléguait que l'information était retenue par le SCC « dans une tentative flagrante pour dissimuler la corruption, le harcèlement et l'inconduite criminelle de bon nombre de ses agents [traduction]. »

Notre enquête a révélé que le SCC n'avait même pas récupéré ni examiné les enregistrements vidéo avant de répondre à la demande du plaignant.

Dix vidéos avaient déjà été détruites en vertu des règles normalisées de conservation du SCC lorsque le détenu a présenté sa demande, mais le SCC ne l'en a pas informé.

Six autres vidéos existaient toujours au moment de la demande du plaignant, mais le SCC n'a fait aucun effort pour les récupérer. Elles ont donc été détruites, elles aussi.

Nous avons conclu que les plaintes concernant ces 16 enregistrements vidéo étaient **fondées**.

Les deux autres vidéos montraient des incidents de recours à la force. En vertu des règles du SCC, de tels enregistrements doivent être conservés pendant au moins 30 jours, contrairement à la période de conservation minimale d'usage de 4,5 jours pour tout autre enregistrement.

Le SCC a cité les deux mêmes dispositions de la *Loi sur la protection des renseignements personnels* pour soustraire ces deux enregistrements, comme pour les 16 autres. Cependant, l'organisation n'a pas examiné les deux enregistrements avant de faire la demande d'exception.

Contrairement aux 16 autres enregistrements qui avaient été détruits, ces deux enregistrements ont pu être examinés par l'enquêteur. Nous avons constaté que les vidéos ne montraient pas d'autres détenus que le plaignant, contrairement à ce que le SCC avait indiqué dans son refus de communiquer les enregistrements. Toutefois, le Commissariat a déterminé que le SCC avait correctement appliqué les autres motifs de refus en démontrant que la communication de l'information pourrait raisonnablement être préjudiciable à la sécurité d'un établissement correctionnel.

Nous avons conclu que les plaintes concernant ces deux enregistrements vidéo étaient **résolues**.

Dans tous les cas, les réponses du SCC sont troublantes, dans la mesure où elles semblent indiquer une approche selon laquelle le refus d'accès est le point de départ pour le traitement des demandes de renseignements personnels aux termes de la *Loi*, plutôt qu'une approche axée sur la transparence et la responsabilité, que la *Loi* a pour but de favoriser. Dans 16 cas, le SCC a appliqué des exceptions à la communication de documents qui n'existaient même pas lorsque le SCC a donné sa réponse. Nous avons recommandé que le SCC prenne des mesures appropriées pour veiller à ce que les demandes de documents présentées en vertu de la *Loi sur la protection des renseignements personnels* se rendent aux responsables compétents à temps pour empêcher la destruction des documents lorsque leur période de conservation est courte.

6.2.2 Le Service correctionnel du Canada refuse de donner accès à l'ensemble du contenu d'un rapport et n'en fournit que « l'essentiel »

Dans une plainte présentée au Commissariat en janvier 2011, un plaignant alléguait que le Service correctionnel du Canada (SCC) avait refusé de lui remettre une copie d'un rapport concernant son traitement et sa supervision. Environ deux mois après

avoir fait la demande d'accès en 2010, le plaignant a reçu un rapport de trois pages comportant deux constatations. Toutefois, lors d'une conversation avec le rédacteur du rapport, le plaignant a appris que le rapport comptait en fait 10 pages, et qu'il comportait 14 constatations. Notre enquête a révélé qu'effectivement, le rapport officiel comptait 10 pages.

Les responsables du SCC ont expliqué que le rapport était fondé sur des entrevues informelles. Il a donc été décidé qu'il serait préférable de soustraire à la communication le rapport plus détaillé et de fournir un document condensé résumant « l'essentiel ».

La version abrégée, à notre avis, constituait une fausse représentation de l'information. La manière dont l'information demandée par le plaignant a été traitée par le Bureau de l'accès à l'information et de la protection des renseignements personnels du SCC allait à l'encontre de la responsabilité de ce dernier qui lui incombe de cerner tous les renseignements pertinents qui existaient au moment où la demande a été reçue et de traiter ces renseignements en conformité avec les dispositions de la *Loi*.

Après de longues négociations, le plaignant a pu obtenir une copie du rapport intégral dans laquelle on avait soustrait certains renseignements personnels concernant d'autres parties. À notre demande, le SCC a également convenu d'effectuer un examen sur le traitement accordé à la demande d'accès et d'informer les employés leurs obligations en vertu de la *Loi sur la protection des renseignements personnels*, notamment au moyen d'un exposé à l'intention du personnel de direction soulignant le rôle important que joue l'organisation pour ce qui est d'assurer le droit à la vie privée.

6.2.3 La Gendarmerie royale du Canada a révélé une absolution inconditionnelle

Afin d'être autorisé à travailler dans un aéroport, un homme a présenté, en juillet 2010, une demande pour la nécessaire habilitation de sécurité en matière de transport. En septembre 2011, Transports Canada a informé l'homme que sa demande d'habilitation de sécurité avait été refusée en raison de renseignements reçus de la part de la Gendarmerie royale du Canada (GRC).

L'homme s'est plaint au Commissariat que la GRC avait communiqué ses renseignements personnels à Transports Canada.

Or, en présentant sa demande d'habilitation de sécurité, le plaignant avait autorisé Transports Canada à obtenir tous les renseignements pertinents, y compris les renseignements figurant dans les dossiers d'application de la loi, et il avait également autorisé toute personne possédant des renseignements relatifs à l'habilitation à communiquer ces renseignements à Transports Canada.

Dans le cadre d'une vérification des dossiers d'application de la loi pour le compte de Transports Canada, la GRC a obtenu de la police de la Colombie-Britannique le résumé d'un incident survenu en 2009 mettant en cause le plaignant. La GRC a ajouté des renseignements selon

lesquels l'incident avait été transféré à une cour provinciale, qui accordait au plaignant une absolution inconditionnelle quelques mois plus tard.

En 2011, la GRC a remis son rapport à Transports Canada, y compris les renseignements relatifs à l'incident et à l'absolution inconditionnelle.

En vertu de la *Loi sur le casier judiciaire*, la GRC n'est pas autorisée à communiquer le dossier d'une absolution inconditionnelle lorsque plus d'une année s'est écoulée, à moins que le ministre responsable de la GRC ait donné son approbation préalable.

Puisqu'une telle approbation n'avait pas été obtenue dans ce cas et que 19 mois s'étaient écoulés depuis l'absolution inconditionnelle, la communication contrevenait à la *Loi sur le casier judiciaire*. Il ne s'agissait pas non plus de l'une des situations de communication limitée de renseignements personnels autorisée par la *Loi sur la protection des renseignements personnels*. Par conséquent, nous avons conclu que la plainte était **fondée**.

Nous avons recommandé que la GRC envoie une lettre d'excuses au plaignant.

6.2.4 Préoccupation soulevée quant à la communication de renseignements personnels en ligne — bande de la Première Nation Qalipu Mi'kmaq

La bande de la Première Nation Qalipu Mi'kmaq, qui a été créée par effet d'un accord conclu entre le gouvernement du Canada et la Fédération des Indiens de Terre-Neuve, a été officiellement établie en 2011. La bande donne un statut officiel aux Mi'kmaq qui sont dispersés aux quatre coins de Terre-Neuve et qui ne peuvent donc pas être décrits en faisant référence aux terres qu'ils occupent collectivement.

L'accord établissant la bande de la Première Nation Qalipu Mi'kmaq prévoyait la mise en place d'un processus d'inscription qui exigeait le nom complet et la date de naissance de tous les membres fondateurs de la bande aux fins de publication dans la *Gazette du Canada*, qui est accessible en ligne.

Une femme, qui avait été reconnue comme membre fondateur, s'est plainte au Commissariat qu'Affaires autochtones et Développement du Nord Canada (AADNC) l'exposait au risque de vol d'identité en publiant à grande échelle des renseignements personnels aussi complets.

Après enquête, nous avons établi que la communication du nom et de la date de naissance de la plaignante était conforme à la disposition de la *Loi sur la protection des renseignements personnels* qui prévoit que les renseignements personnels peuvent être communiqués sans le consentement de l'individu, lorsque ces renseignements servent aux fins auxquelles ils ont été recueillis à l'origine.

En outre, la communication servait à identifier et à reconnaître les membres de la bande, ce qui était la raison même pour laquelle les renseignements personnels ont initialement été recueillis sur les formulaires d'inscription.

Nous avons conclu que la plainte était **non fondée**. Étant donné que le vol d'identité est un risque réel dans l'environnement électronique d'aujourd'hui, nous avons toutefois demandé à AADNC d'envisager d'autres solutions dans l'avenir. On pourrait notamment demander de ne fournir qu'une date de naissance partielle ou permettre d'établir un lien par un autre identificateur à un registre hors ligne qui contient la date de naissance.

6.2.5 Réception des plaintes

Une unité spéciale de réception des plaintes est chargée d'analyser, de trier et d'enregistrer toutes les plaintes écrites relatives à la protection de la vie privée qui sont soumises au Commissariat. Cette unité joue un rôle essentiel en aidant le Commissariat à comprendre les préoccupations et les attentes des plaignants.

Toutes les plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels* sont envoyées à cette unité. Après un examen initial de la plainte, l'équipe responsable de la réception des plaintes fait un suivi auprès du plaignant, au besoin, afin d'obtenir des précisions et tout autre renseignement nécessaire à la tenue d'une enquête.

L'équipe responsable de la réception des plaintes a connu un succès considérable pour ce qui est de régler immédiatement certains problèmes de protection de la vie privée, ce qui élimine la nécessité pour les personnes de se soumettre à de longues enquêtes plus officielles.

6.2.6 Plaintes

Pour la deuxième année consécutive, il y a eu une augmentation du nombre de plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées par le Commissariat. Pour 2012-2013, le total était de 2 273, ce qui représentait le nombre le plus élevé à ce jour et une augmentation de 133 % par rapport à l'exercice précédent.

Toutefois, ce total record était cependant gonflé par 1 159 plaintes découlant de deux atteintes à la protection des données mettant en cause Ressources humaines et Développement des compétences Canada[7] et le ministère de la Justice Canada. Étant donné que la commissaire a déposé ses propres plaintes dans ces dossiers, les personnes concernées n'ont pas eu besoin de le faire pour déclencher une enquête officielle; malgré tout, bien des gens ont choisi de déposer une plainte.

Si on enlève les 1 159 plaintes déposées en lien avec ces deux atteintes à la protection des données, il reste 1 114 plaintes. De ce nombre, 251 (20 %) se résumaient à huit plaintes ou plus provenant de 18 personnes. Au cours des trois années précédentes, près des trois quarts de tous les plaignants ont déposé plus d'une plainte.

[7] Ressources humaines et Développement des compétences Canada (RHDCC) a depuis été renommé Emploi et Développement social Canada. Toutefois, aux fins du présent rapport, nous utilisons le nom que portait le Ministère au moment des incidents et tout au long de la période de rapport.

La plupart de ces nombreuses plaintes étaient liées à une détérioration des relations employeur-employé au sein des institutions fédérales. Dans le cadre du projet de modernisation décrit plus loin dans le présent chapitre, des stratégies sont élaborées en vue de rationaliser les nombreuses plaintes portées par le même plaignant.

En règle générale, les problèmes employeur-employé sous-jacents et les griefs des employés appuyés par les syndicats relatifs au milieu de travail ont également contribué à augmenter le nombre de plaintes.

Nous avons aussi constaté une augmentation des plaintes de la part de membres de la fonction publique fédérale liées à la communication de leurs renseignements personnels à des tiers fournisseurs de services.

Il y a également eu une augmentation du nombre de plaintes et d'atteintes à la protection des données en raison d'un accès inapproprié par les employés ou de vulnérabilités dans les technologies de l'information.

Les plaintes, qui peuvent être déposées pour diverses raisons en vertu de la *Loi sur la protection des renseignements personnels*, appartiennent à trois catégories distinctes : accès, protection des renseignements personnels et délais. Ces catégories sont décrites à l'annexe 1. Des statistiques détaillées sur les plaintes figurent à l'annexe 3.

6.2.7 Règlement rapide

Quand il est couronné de succès, le processus de règlement rapide constitue la meilleure solution pour toutes les parties concernées. Pour les personnes qui déposent une plainte en vertu de la *Loi sur la protection des renseignements personnels*, cela signifie qu'elles obtiennent rapidement les réponses qu'elles cherchent. Pour les institutions fédérales, cela veut dire qu'elles évitent un processus qui est souvent long et coûteux en ressources.

Essentiellement, le règlement rapide repose habituellement sur la négociation et la conciliation plutôt que sur une enquête plus officielle.

Toutes les plaintes sont examinées dès leur réception pour savoir s'il y a possibilité de règlement rapide. Il faut tenir compte de la complexité apparente du cas et déterminer s'il semble évoquer des questions déjà abordées.

Les plaignants sont souvent satisfaits d'une explication sur les renseignements que les ministères peuvent légalement soustraire à la communication en vertu des exceptions prévues par la *Loi*. En outre, s'il a été déterminé que des ministères dans des situations similaires respectaient la *Loi sur la protection des renseignements personnels*, les plaignants éventuels conviennent souvent qu'il y a peu d'intérêt à aller de l'avant avec une enquête officielle.

Au cours des dernières années, le taux de succès du processus de règlement rapide a connu une croissance continue. En 2012-2013, nous avons réglé plus

du tiers de toutes les plaintes reçues au moyen du processus de règlement rapide, comparativement à un quart au cours de l'exercice précédent.

6.2.8 Modernisation du processus d'enquête

Le processus utilisé par le Commissariat pour enquêter sur les plaintes en vertu de la *Loi sur la protection des renseignements personnels* est soumis à des pressions accrues en raison de la hausse du volume de plaintes. Le Commissariat en est en outre venu à apprécier la valeur du passage d'un modèle qui était fondé en grande partie sur les positions des parties à un modèle qui accorde davantage d'attention à répondre aux intérêts de toutes les parties.

En 2012, ces deux facteurs ont alimenté un projet visant à moderniser le processus d'enquête. Ce projet a donné lieu à l'établissement d'une série de mesures qui, à notre avis, permettront d'améliorer nos services aux Canadiennes et aux Canadiens tout en réduisant le temps et les ressources nécessaires pour enquêter sur des plaintes complexes et potentiellement systémiques.

Quatre priorités ont guidé le projet :

- renforcer l'étape initiale de la réception des plaintes, qui joue un rôle de contrôle, et améliorer l'approche de règlement rapide qui, si elle convient, peut éliminer la nécessité d'effectuer une enquête plus officielle;
- adopter une approche de médiation pour les enquêtes sur les plaintes qui est axée sur les résultats finaux et qui prend en considération les intérêts sous-jacents aux positions des parties;
- renforcer les relations avec les institutions fédérales afin de faciliter l'échange de renseignements et d'accélérer le temps de réponse;
- modifier le processus d'enquête afin de le simplifier et d'en accroître l'efficience.

L'essentiel d'une bonne partie des efforts de modernisation a consisté à veiller à ce que les différentes procédures utilisées soient proportionnelles aux défis à relever, car, comme le dit la sagesse populaire, on ne tue pas une mouche avec un canon.

Par exemple, les atteintes à la sécurité des renseignements personnels seront désormais analysées au moment de leur signalement afin de déterminer si leur incidence sera faible, moyenne ou élevée. L'incidence sera déterminée selon le degré de préjudice potentiel pour les parties concernées ou le public, le risque de récurrence, les contrôles en place et les mesures prises pour prévenir ou corriger le problème, ainsi que le niveau de communication. Le processus d'enquête sera adapté au niveau d'incidence.

Le nombre de plaintes présentées au Commissariat contre les institutions fédérales qui ne respectent pas les délais prévus par la *Loi* pour le traitement des demandes de renseignements personnels de particuliers a récemment augmenté de façon importante. Cette augmentation est souvent

attribuable au fait que les institutions doivent composer avec un volume plus élevé de demandes de renseignements personnels sans pour autant disposer du personnel nécessaire.

Afin de répondre à cette situation, l'équipe du projet de modernisation a élaboré une nouvelle stratégie pour traiter les plaintes relatives aux délais, laquelle est aussi fondée sur le respect des proportions. La première mesure à prendre consistera à tenter d'obtenir un règlement rapide. (Voir l'explication fournie plus tôt dans la présente section.)

Les autres approches vont de l'émission rapide d'une présomption de refus au règlement de la plainte à la satisfaction du plaignant, dans la mesure du possible.

Voici d'autres innovations découlant du projet de modernisation en ce qui a trait aux processus :

- remplacer le courrier ordinaire par des courriels cryptés, lorsque cela est possible sur le plan technique, pour des communications plus rapides avec 14 institutions qui comptent un grand volume de plaintes;
- assigner un « portefeuille » d'institutions à chacune des équipes d'enquêteurs afin de leur permettre d'acquérir et de développer une expertise au sujet de ces institutions, tout en réduisant au minimum le nombre d'enquêteurs avec lesquels chaque institution doit traiter. Cette approche permettra en outre de cerner plus efficacement les enjeux systémiques et de les gérer efficacement;
- affecter un seul enquêteur au traitement des plaintes multiples provenant d'une même personne et en rendre compte dans un seul rapport, dans la mesure du possible.

La mise en œuvre du processus de modernisation se poursuit et d'autres améliorations possibles sont examinées.

6.2.9 Enquêtes et décisions — des chiffres

Plusieurs enquêtes importantes sur des plaintes sont décrites en détail aux chapitres 2 et 3. La présente section examine la situation globale qui se cache derrière les chiffres. Des statistiques détaillées figurent à l'annexe 3.

En 2012-2013, le nombre de plaintes acceptées par le Commissariat a plus que doublé par rapport au dernier exercice, soit 2 273 comparativement à 986. Cette augmentation sans précédent a été engendrée par 1 159 nouvelles plaintes découlant des deux atteintes à la sécurité des renseignements personnels qui se sont produites à Ressources humaines et Développement des compétences Canada.

Au total, 908 plaintes ont été fermées au cours de l'année, dont le tiers au moyen du processus de règlement rapide. Au cours de l'année précédente, le Commissariat a fermé 913 dossiers, dont près du quart au moyen du processus de règlement rapide.

Les problèmes d'accès ont été l'élément déclencheur pour plus de 70 % des plaintes non fondées. En

règle générale, les personnes contestaient le refus d'une institution de leur accorder l'accès à leurs renseignements personnels. Dans la plupart des cas, toutefois, nous avons constaté que les exceptions appropriées avaient été appliquées ou que l'institution avait effectué une recherche raisonnable pour obtenir l'information, et nous étions convaincus qu'il n'existait pas d'autres documents pertinents. Le nombre de plaintes fondées visant le secteur public continue d'être considérablement plus élevé que celui des plaintes visant le secteur privé. En 2012-2013, environ les trois quarts des plaintes fondées en vertu de la *Loi sur la protection des renseignements personnels* visaient des institutions n'ayant pas donné suite à des demandes d'accès dans les délais prévus par la *Loi*.

DÉCISIONS*	Nombre de cas	Pourcentage
Non fondée	166	18
Fondée	276	30,5
Réglée rapidement	299	33
Abandonnée	60	7
Réglée en cours d'enquête	33	4
Fondée et résolue	47	5
Résolue	22	2
Hors du champ d'application	5	0,5
Total	908	100

* Les définitions des décisions sont fournies à l'annexe 1. Pour une ventilation plus détaillée, prière de consulter le tableau intitulé « Décision par type de plainte », à l'annexe 3.

Après avoir connu une diminution entre les deux périodes de rapport précédentes, le délai de traitement moyen nécessaire pour clore les enquêtes officielles, à l'exclusion de toutes les autres, a augmenté légèrement en 2012-2013, passant de 7,6 mois en 2011-2012 à 8,3 mois en 2012-2013.

Les délais de réponse des ministères et organismes étaient à l'origine d'une partie de cette hausse, tout comme l'augmentation du nombre de plaintes complexes. La catégorie des plaintes complexes liées à l'utilisation, à la communication, à la collecte et à la conservation des renseignements personnels, qui représentait 22 % des plaintes donnant lieu à une enquête officielle l'année précédente, est passée à 64 % cette année.

Le perfectionnement de notre approche de règlement rapide nous a toutefois permis de faire en sorte que le délai moyen requis pour clore un dossier demeure assez court. Le délai de traitement combiné pour les enquêtes officielles et le règlement rapide a atteint 6,7 mois en 2012-2013. Même si cela représente une augmentation de 15 % par rapport aux 5,8 mois de l'an dernier, c'est quand même plus rapide que pour les trois années précédentes, où les délais ont été de 19,5 mois en 2008-2009, 12,9 mois en 2009-2010 et 7,2 mois en 2010-2011.

Lors de ces années antérieures, le Commissariat calculait le délai de traitement à partir de la date de réception de la plainte, même s'il manquait des renseignements essentiels dans le dossier et qu'il fallait demander des précisions avant de pouvoir commencer le travail. Depuis 2011, les plaintes ne sont considérées comme « acceptées » qu'une fois que le dossier est complet. Nous estimons que cette définition donne une idée plus juste des délais de traitement.

Cela signifie qu'à partir de l'exercice 2011-2012 les statistiques relatives aux plaintes ont été compilées différemment des exercices précédents. Pour les pourcentages, cela ne fait pas beaucoup de différence.

Plus de 90 % de toutes les plaintes acceptées en 2012-2013 provenaient des dix institutions ayant fait l'objet du plus grand nombre de plaintes, ce qui constitue une légère augmentation par rapport au pourcentage dans la mi-80 des trois derniers exercices.

Cependant, les ministères qui font partie de la liste des dix institutions ayant fait l'objet du plus grand nombre de plaintes ne sont pas les mêmes que l'an dernier :

- Ressources humaines et Développement des compétences Canada, qui se classait en 8e place, occupe maintenant la première.
- L'Agence du revenu du Canada est passée de la 4e place à la 7e place.
- Certaines institutions figurent au palmarès pour la première fois cette années. C'est le cas de Justice Canada, qui occupe la 3e place, de l'Agence canadienne d'inspection des aliments, qui occupe la 9e place, et de Transports Canada, qui occupe la 10e place.
- Le Service canadien du renseignement de sécurité, Travaux publics et Services gouvernementaux Canada et Postes Canada ne font pas partie de la liste cette année.

Les dix institutions ayant fait l'objet du plus grand nombre de plaintes acceptées en 2012-2013

Institution	
Ressources humaines et Développement des compétences Canada	1 030
Service correctionnel du Canada	284
Ministère de la Justice Canada	188
Gendarmerie royale du Canada	182
Ministère de la Défense nationale	90
Agence des services frontaliers du Canada	88
Agence du revenu du Canada	76
Anciens Combattants Canada	56
Agence canadienne d'inspection des aliments	33
Transports Canada	27
Tous les autres ministères et organismes	219

6.3 VÉRIFICATIONS

La *Loi sur la protection des renseignements personnels* donne à la commissaire le pouvoir de mener, à sa discrétion, des vérifications des pratiques des ministères et des organismes fédéraux en ce qui concerne le traitement des renseignements personnels. Si une vérification révèle des lacunes, la commissaire peut recommander des mesures de correction à l'institution en cause.

Les conclusions et les recommandations des vérifications peuvent être publiées dans un rapport annuel ou dans un rapport spécial au Parlement. Outre cette communication publique, la *Loi* ne prévoit pas d'autres pouvoirs d'application. Généralement, environ deux ans après la publication d'une vérification, nous assurons un suivi pour déterminer si l'organisation a donné suite à nos recommandations et tenu ses engagements.

Cette année, nous avons procédé au suivi de nos vérifications de 2010 sur les pratiques d'élimination des renseignements et l'utilisation des technologies sans fil au sein d'institutions fédérales choisies.

Nous sommes heureux d'indiquer que les 34 recommandations formulées dans le cadre de ces deux vérifications qui ont été acceptées par les institutions ont été pleinement ou en grande partie mises en œuvre.

6.3.1 Suivi de la vérification des pratiques de retrait

Contexte

Les institutions fédérales recueillent de grandes quantités de renseignements personnels à l'appui de politiques publiques et de l'exécution de programmes et de services. Lorsque des dossiers sans intérêt archivistique ou historique atteignent la fin de leur période de conservation prévue, ou lorsque des données sont conservées sur des ordinateurs obsolètes, l'information est éliminée.

En vertu de la *Loi sur la protection des renseignements personnels*, les institutions fédérales sont tenues de protéger les renseignements destinés à l'élimination avec le même soin qu'elles accordent aux renseignements contenus dans leurs dossiers courants. Il en va de la confiance du public à l'égard de la capacité du gouvernement de protéger les renseignements personnels sensibles.

L'absence de mesures de contrôle adéquates en ce qui a trait à l'élimination des documents dont le gouvernement n'a plus besoin a été au cœur de l'une des atteintes à la protection des renseignements personnels les plus monumentales dont le Commissariat a eu connaissance. En 1998, le Commissariat a découvert que quatre camions pleins de documents confidentiels intacts du gouvernement fédéral renfermant des renseignements personnels allaient être envoyés aux États-Unis, en Corée

du Sud et en Chine. L'entreprise privée qui avait obtenu le contrat de déchiquetage et de recyclage des documents les exportait plutôt tels quels parce que, sur le marché du recyclage, la vente de papier intact rapportait davantage que la vente de papier déchiqueté.

À l'époque, nous avons recommandé que Bibliothèque et Archives Canada (BAC) ait recours à des services de déchiquetage hors site seulement si l'entreprise retenue pouvait garantir que des mesures de sécurité adéquates seraient prises et que le déchiquetage serait effectué sous surveillance constante.

Au moment de la vérification initiale, BAC offrait des services d'entreposage et de destruction des documents à plus de 90 ministères et organismes fédéraux. Nous avons examiné son programme de destruction de papier de rebut à l'extérieur du Ministère et les ententes contractuelles avec les entreprises de déchiquetage privées.

Nous avons également examiné la distribution d'ordinateurs excédentaires donnés dans le cadre du Programme des ordinateurs pour les écoles du gouvernement du Canada, qui est exécuté par des organismes sans but lucratif en vertu d'ententes conclues avec Industrie Canada (IC).

La vérification

À l'issue de notre vérification, qui a pris fin en octobre 2010, nous avons conclu que BAC possédait un ensemble complet de politiques, de procédures et de processus pour gérer la destruction des documents du gouvernement fédéral. Les exigences en matière de sécurité intégrées aux contrats de destruction hors site étaient conformes aux politiques du gouvernement et elles prévoyaient des mesures de contrôle afin d'assurer le transport, l'entreposage et la destruction de documents de façon sécuritaire.

Toutefois, nous avons également constaté ce qui suit :

- La destruction hors site de documents ne faisait pas l'objet d'une surveillance systématique — au moyen d'inspections et de vérifications périodiques — visant à faire en sorte que les exigences en matière de protection de la vie privée et de sécurité soient respectées de façon uniforme.
- Il n'y avait pas de critères uniformes relatifs au déchiquetage afin de rendre impossible la reconstitution de renseignements figurant sur du papier déchiqueté.

Le Programme des ordinateurs pour les écoles est géré par IC. Dans le cadre du Programme, on fait la collecte et la remise à neuf d'ordinateurs excédentaires reçus du gouvernement et du secteur privé aux fins de distribution dans des écoles, des bibliothèques publiques, des communautés autochtones et des organismes d'enseignement sans but lucratif de partout au Canada.

Selon la politique du Secrétariat du Conseil du Trésor du Canada, les ministères et organismes fédéraux doivent supprimer tous les renseignements classifiés et protégés enregistrés sur les ordinateurs

excédentaires avant de les donner au Programme des ordinateurs pour les écoles. Nous avons constaté que les ordinateurs en provenance de 28 des 31 institutions fédérales que nous avons visitées (90 %) ne satisfaisaient pas à cette exigence.

Nous avons également constaté qu'IC n'avait établi aucun protocole pour l'analyse et le traitement des lacunes en matière de sécurité qui lui sont signalées par les centres de remise à neuf du Programme des ordinateurs pour les écoles.

Le suivi

BAC et IC signalent que les quatre recommandations de la vérification de 2010 ont été entièrement mises en œuvre.

Les responsables du Programme des ordinateurs pour les écoles ont élaboré un nouveau rapport d'attestation du matériel excédentaire. Tous les dons d'ordinateurs s'accompagnent d'une déclaration signée attestant que le matériel offert est complet et en bon état de fonctionnement, et que toute information protégée contenue sur les lecteurs de disque dur de tous les ordinateurs et ordinateurs portatifs présentés dans le rapport a été effacée de façon électronique.

En outre, chaque centre de remise à neuf soumet annuellement un questionnaire révisé sur la sécurité, qui est analysé afin de cerner et de corriger les lacunes ou les faiblesses potentielles en matière de sécurité.

BAC a confirmé que tous les contrats accordés pour des services de destruction de documents hors site comprennent des critères de déchiquetage qui répondent aux exigences du gouvernement fédéral en matière de sécurité. Les contrats comprennent également des clauses types afin d'assurer un niveau approprié d'activités de surveillance périodique.

De plus, les fournisseurs de services doivent émettre des certificats de destruction, indiquant la date à laquelle les fichiers ont été détruits et le nom de l'employé de l'entrepreneur autorisé qui a effectué la destruction ou qui en a été témoin.

6.3.2 Suivi de la vérification de l'utilisation des technologies sans fil

Contexte

Des dizaines de milliers de fonctionnaires fédéraux ont reçu des téléphones intelligents ou d'autres dispositifs portatifs avec lesquels ils peuvent effectuer des communications vocales ou des transmissions de données. Certains ministères et organismes utilisent des réseaux sans fil afin de permettre aux fonctionnaires qui disposent d'ordinateurs portatifs ou d'autres dispositifs mobiles de se brancher à leurs ordinateurs de bureau.

Ces technologies sans fil offrent flexibilité et commodité, mais elles présentent également des risques liés à la protection de la vie privée.

Cinq organisations avaient été sélectionnées pour la vérification : la Société canadienne d'hypothèques

et de logement; le Service correctionnel du Canada; Santé Canada; Ressources humaines et Développement des compétences Canada; Affaires autochtones et Développement du Nord Canada (alors connue sous le nom d'Affaires indiennes et du Nord Canada).

La vérification

Notre vérification, qui a également pris fin en octobre 2010, a permis de constater que les cinq institutions choisies avaient adopté des politiques, procédures et processus de gestion des renseignements personnels transmis et conservés dans leurs environnements sans fil. Le Commissariat a toutefois cerné des faiblesses devant être corrigées, notamment :

- aucune des entités n'avait vraiment évalué les menaces et les risques associés aux technologies sans fil;
- seulement trois des cinq institutions avaient adopté des protocoles de protection par mot de passe robuste pour les téléphones intelligents;
- aucune des institutions n'avait défini une exigence voulant que les données conservées dans la mémoire de ces dispositifs soient cryptées;
- quatre des cinq institutions ne disposaient pas de procédures documentées visant à limiter le risque d'une atteinte à la protection des données en cas de perte ou de vol d'un dispositif;
- à une seule exception, les institutions ne sensibilisaient généralement pas les utilisateurs des dispositifs sans fil à la manière de les utiliser de façon à protéger la vie privée.

Nous avons également constaté que toutes les institutions soumises à la vérification autorisaient la messagerie NIP à NIP ou messagerie de « poste à poste ». Pourtant, aucune n'a pu démontrer qu'elle avait adopté des mesures pour traiter des enjeux de sécurité afférents à l'utilisation de cette méthode de communication, comme le recommandait le Centre de la sécurité des télécommunications Canada (CSTC). Finalement, nous avons noté des faiblesses dans la gestion des dispositifs sans fil excédentaires.

Le suivi

Nous avons fait un suivi auprès des cinq institutions afin de déterminer si elles avaient donné suite à leurs engagements quant à nos recommandations. Sur les 30 recommandations de la vérification, qui ont été acceptées collectivement, les institutions ont indiqué que 29 avaient été entièrement mises en œuvre; la recommandation restante a été mise en œuvre en grande partie. Les mesures correctrices comprennent ce qui suit :

- effectuer des évaluations de la menace et des risques sur les réseaux sans fil;
- intégrer les risques pour la protection de la vie privée et les techniques d'atténuation de ces risques aux diverses initiatives de sensibilisation du personnel;

- officialiser les processus relatifs à la perte et au vol des dispositifs sans fil;
- mettre en œuvre des politiques de protection par mot de passe et de cryptage des données;
- mettre en œuvre des politiques et des processus pour restreindre l'utilisation de la messagerie NIP à NIP;
- instaurer des mécanismes pour s'assurer que les données conservées dans les dispositifs sans fil excédentaires soient effacées avant l'élimination de ces dispositifs.

Les mesures mises en œuvre par les cinq institutions pour donner suite à nos recommandations permettront d'atténuer les risques pour la vie privée que posent les technologies et les dispositifs sans fil.

6.4 DEMANDES DE RENSEIGNEMENTS

Notre Centre d'information répond aux demandes de renseignements du grand public et des organisations sur les droits et responsabilités liés à la protection de la vie privée. En 2012-2013, nous avons reçu près de 10 000 demandes de renseignements.

Plus de 25 % des demandes de renseignements étaient liées à la *Loi sur la protection des renseignements personnels* et portaient sur un vaste éventail de questions. Certaines des questions les plus fréquentes étaient les suivantes : la façon dont les personnes peuvent s'y prendre pour avoir accès aux renseignements personnels les concernant qui sont détenus par les ministères; le processus relatif aux plaintes du Commissariat; l'application de la *Loi* en cas de perte de renseignements ou de communication accidentelle.

Près du tiers des demandes portaient sur des questions qui ne sont pas du ressort du Commissariat. Dans de tels cas, nous offrons de l'aide en dirigeant les personnes vers d'autres organisations ou en proposant des façons de régler les problèmes ou de trouver l'information recherchée.

6.5 APPUI AU PARLEMENT

Comparutions devant le Parlement

En 2012-2013, la commissaire, la commissaire adjointe et d'autres représentants du Commissariat ont comparu officiellement neuf fois devant les députés et les sénateurs. Nous avons également présenté deux mémoires écrits aux comités parlementaires.

Parmi les questions abordées, mentionnons :

- les répercussions sur la protection de la vie privée découlant des mesures de sécurité frontalière visant les voyageurs dans le projet de loi omnibus C-45 (détails au chapitre 5);
- le nouveau projet de loi sur la transparence financière des Premières Nations (projet de

loi C-27) et des syndicats (projet de loi C-377) (détails ci-dessous);

- les modifications au *Code criminel* limitant les interceptions effectuées sans mandat par la police dans des situations d'urgence, également dans le projet de loi C-55 (détails au chapitre 5);
- le Budget principal des dépenses du Commissariat;
- l'étude spéciale sur les médias sociaux menée par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) devant lequel nous avons comparu à deux reprises;
- les rapports annuels concernant la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), également devant le Comité ETHI.

6.5.1 Obligation redditionnelle et transparence des Premières Nations en matière financière

En vertu du projet de loi C-27, *Loi visant à accroître l'obligation redditionnelle et la transparence des Premières Nations en matière financière*, les chefs et les conseillers des Premières Nations doivent remettre chaque année une annexe vérifiée des rémunérations au ministre des Affaires autochtones et du Développement du Nord Canada.

Cette annexe indique tous les paiements versés par une Première Nation, ou par toute entité qu'elle contrôle, à son chef et à chacun de ses conseillers, qu'ils agissent à titre professionnel ou personnel. Le projet de loi exige en outre que les Premières Nations publient cette annexe sur leur site Web et qu'elles en fournissent des copies sur demande. De plus, le ministre est tenu de publier les annexes sur le site Web du Ministère.

Lors de sa comparution devant le Comité permanent des affaires autochtones et du développement du Grand Nord de la Chambre des communes, la commissaire a indiqué aux membres du Comité que la *Loi sur la protection des renseignements personnels* autorise la divulgation de renseignements personnels sans consentement dans les cas où une autre loi du Parlement autorise une telle divulgation (en l'occurrence le projet de loi C-27).

Ainsi, il n'était pas question de la légalité du projet de loi, mais plutôt de trouver un équilibre entre deux principes démocratiques d'importance égale, soit l'obligation redditionnelle et la protection des renseignements personnels. La commissaire a énuméré plusieurs éléments dont le Comité peut tenir compte pour ce qui est d'évaluer la proportionnalité du projet de loi et d'envisager des options qui portent moins atteinte à la vie privée. Dans l'ensemble, la commissaire a présenté au Comité un cadre d'analyse en quatre étapes pour trouver le juste équilibre entre l'atteinte des objectifs déterminés de la politique et la protection de la vie privée.

Le cadre peut se résumer en quatre grandes questions au sujet d'une initiative ou d'un programme du gouvernement.

La première question permet d'évaluer si une mesure proposée dans le cadre d'une initiative ou d'un programme est nécessaire pour atteindre les objectifs déterminés de la politique.

La deuxième question examine si la mesure proposée permettra efficacement d'atteindre l'objectif déterminé de la politique. Il se peut que la mesure proposée ne soit pas particulièrement efficace pour l'atteinte des objectifs pour lesquels elle a été élaborée.

La troisième question, axée sur la proportionnalité, prend sensiblement la forme d'un critère de pondération qui permet de déterminer si les effets bénéfiques de la mesure proposée sont plus importants que les effets préjudiciables sur la vie privée des personnes.

Finalement, la quatrième question demande si la mesure proposée peut être remplacée par une autre mesure qui aurait des répercussions moins néfastes sur la vie privée.

Le projet de loi a reçu la sanction royale le 27 mars 2013.

6.5.2 Exigences applicables aux organisations ouvrières de la *Loi de l'impôt sur le revenu*

Le projet de loi d'initiative parlementaire C-377 a été présenté à la Chambre des communes, le 5 décembre 2011, par le député conservateur Russ Hiebert. Le projet de loi modifierait la *Loi de l'impôt sur le revenu* afin d'exiger que, dans les six mois suivant la fin de chaque exercice, les organisations ouvrières et les fiducies de syndicat présentent au ministre du Revenu national une déclaration publique de renseignements pour l'exercice.

Le ministre serait alors tenu de communiquer au public les renseignements contenus dans ces déclarations, notamment en les publiant sur le site Internet du Ministère dans un format permettant la recherche par mot et les renvois croisés entre les données.

Le 7 novembre 2012, la commissaire a comparu devant le Comité permanent des finances au sein d'un groupe d'experts formé de sept autres participants. Elle a indiqué que le projet de loi C-377 soulevait d'importantes préoccupations en matière de protection de la vie privée et, comme pour le projet de loi C-27, elle a proposé le cadre d'analyse en quatre étapes pour évaluer si le projet de loi permettait de trouver le juste équilibre entre la transparence et la responsabilité, d'une part, et le droit à la vie privée des personnes, d'autre part.

Dans sa comparution devant le Comité, le 25 octobre 2012, M. Hiebert a proposé des modifications à son projet de loi qui auraient permis d'atténuer les dispositions portant atteinte à la vie privée. Cependant, puisque le Comité n'a pas présenté ses conclusions à la Chambre des communes avant la fin d'une prorogation de 30 jours, le projet de loi C-377 a été réputé avoir fait l'objet d'un rapport sans amendement, le 27 novembre 2012.

Le 7 décembre 2012, à la Chambre des communes, M. Hiebert et l'opposition ont présenté de nouveau plusieurs amendements visant divers enjeux découlant du projet de loi C-377; seuls les amendements présentés par le député ont été adoptés. Certains portaient sur des questions relatives à la protection de la vie privée, dont un visant à éliminer le risque de communiquer des renseignements personnels sur les personnes qui touchent des prestations de soins de santé, une pension ou d'autres types de prestations au titre d'un régime enregistré de prestations. Un autre des amendements adoptés avait pour objet de retirer les adresses domiciliaires des exigences en matière de déclaration.

La commissaire a comparu de nouveau relativement au projet de loi C-377 à la suite de son renvoi, en mai 2013, au Comité sénatorial permanent des banques et du commerce. Elle a alors mentionné être plus à l'aise avec la version amendée du projet de loi et a offert des occasions de clarifier davantage l'intention du législateur.

À la fin juin, le Sénat a adopté un amendement qui éliminait les principales dispositions du projet de loi C-377. L'avenir du projet de loi était incertain au moment de la rédaction du présent rapport.

Autres activités parlementaires

En 2012-2013, le Commissariat a examiné huit projets de loi et trois études de comités afin d'analyser les répercussions que le projet de loi et les recommandations des rapports des comités (p. ex. cyberintimidation, médias sociaux, etc.) pourraient avoir sur la protection de la vie privée. Nous avons eu plus de 52 échanges officiels avec les parlementaires et les greffiers, notamment dans le cadre du suivi de nos comparutions devant les comités, d'examens de sujets particuliers avec les députés et les sénateurs, de réunions en personne et de séances d'information technique.

6.6 SENSIBILISATION

Une partie essentielle de notre travail dans le secteur public est de sensibiliser, dans la plus grande mesure possible, les 250 institutions fédérales qui relèvent de la *Loi sur la protection des renseignements personnels*.

Nous visons à promouvoir l'importance d'aviser le Commissariat des atteintes à la vie privée, à aider les institutions fédérales à régler les questions en suspens concernant la protection de la vie privée et à clarifier nos attentes relativement aux évaluations des facteurs relatifs à la vie privée (EFVP).

6.6.1 Atelier sur les EFVP

Pour la quatrième année consécutive, nous avons organisé un atelier sur les EFVP, auquel ont assisté plus de 60 représentants d'institutions fédérales chargés de la protection des renseignements personnels.

L'atelier de cette année, qui revêtait un nouveau format, comportait deux discussions en groupe, dont l'accent était mis sur le respect de la vie privée et la sécurité en lien avec les technologies de l'information (TI), ainsi que sur les EFVP pluri-institutionnelles.

Des experts du Centre de la sécurité des télécommunications Canada et du Commissariat étaient sur place pour répondre aux questions liées à la sécurité et à la protection de la vie privée dans le cadre des TI. Des représentants de Citoyenneté et Immigration Canada, la Gendarmerie royale du Canada et l'Agence des services frontaliers du Canada ont offert aux participants des conseils pratiques élaborés à la suite de la coordination et de la réalisation d'une EFVP pluri-institutionnelle dans le cadre du Projet de biométrie pour les résidents temporaires.

Le Commissariat est flatté du nombre de fonctionnaires fédéraux qui veulent assister à ses grands ateliers. Cependant, à l'avenir, nous prévoyons tenir de plus petites séances sur les EFVP portant sur des sujets plus spécialisés. Cela nous permettra également d'adapter ces séances aux représentants débutants et avancés chargés de la protection des renseignements personnels.

Pour nous aider dans l'élaboration de ces petites séances sur les EFVP, nous avons mené un sondage en décembre 2012 afin d'évaluer le niveau d'expérience en matière d'EFVP dans les institutions fédérales, et d'évaluer les besoins et les intérêts de la communauté de la protection de la vie privée en matière d'EFVP. Nous avons reçu de précieux commentaires au moyen des 121 sondages qui ont été remplis.

6.6.2 Sensibilisation à l'accès à l'information et à la protection des renseignements personnels

Nous sommes toujours heureux de constater la popularité du déjeuner communautaire que nous organisons avec le Commissariat à l'information du Canada à l'intention des professionnels de l'accès à l'information et de la protection des renseignements personnels (AIPRP) dans les institutions fédérales. Des professionnels de l'AIPRP provenant de 46 institutions ont pris part au déjeuner en février.

Nous croyons que l'activité a permis de renforcer la relation avec la communauté de l'AIPRP tant pour le Commissariat à la protection de la vie privée que pour le Commissariat à l'information. Les professionnels de l'AIPRP en ont profité pour partager des expériences et échanger des idées, et pour rencontrer la commissaire et la commissaire adjointe à la protection de la vie privée.

Le Commissariat a tenu des consultations plus ciblées avec les professionnels de l'AIPRP et d'autres représentants des 12 institutions fédérales qui font l'objet du plus grand nombre de plaintes concernant la protection des renseignements personnels. Au printemps, nous avons entrepris avec eux des discussions sur nos initiatives visant à moderniser le processus d'enquête du Commissariat. Nous avons sollicité des commentaires et échangé des pratiques exemplaires.

Nous avons aussi exposé les grandes lignes du projet de modernisation en décembre 2012, lors d'une réunion avec la communauté de l'AIPRP convoquée par le Secrétariat du Conseil du Trésor du Canada.

6.6.3 Discours et exposés

La commissaire Stoddart a présenté des exposés au personnel de la Bibliothèque du Parlement et devant un rassemblement de sous-ministres fédéraux, où elle a expliqué les principales façons dont le Commissariat collabore avec les institutions fédérales, tout en soulignant les grandes tendances en matière de protection des renseignements personnels dans l'ensemble du secteur public. Parmi les thèmes principaux figurait la question de l'accès inapproprié aux renseignements personnels, qui est examinée en profondeur au chapitre 3.

À la suite du signalement de deux atteintes à la vie privée, la commissaire adjointe, Chantal Bernier, a accepté une invitation à prendre la parole devant les gestionnaires et les employés de Ressources humaines et Développement des compétences Canada, à la fin janvier. La commissaire adjointe a attiré l'attention sur l'importance de la protection des données et a offert des conseils sur les pratiques fondamentales que les organisations responsables devraient observer.

En février, la commissaire adjointe a présenté un exposé aux gestionnaires du portefeuille de Sécurité publique Canada, Défense nationale et Citoyenneté et Immigration Canada au ministère de la Justice Canada, où elle a abordé l'interface entre les questions de sécurité et de protection de la vie privée.

Dans un même ordre d'idées, en mars, la commissaire Stoddart a accepté une invitation à s'adresser à l'équipe de la haute direction de l'Agence des services frontaliers du Canada, en avril. L'invitation faisait suite à une lettre que la commissaire a envoyée au président de l'ASFC, dans laquelle étaient soulevées des questions liées à la présentation tardive au Commissariat de l'EFVP portant sur la phase I du système de contrôle des entrées et des sorties (ce point est abordé au chapitre 5) ainsi que des préoccupations relativement à l'intention de l'Agence de mettre en place une surveillance audio dans les aéroports et à son questionnaire sur l'intégrité (les deux points sont abordés plus haut au chapitre 6).

6.7 RECHERCHE

Pour relever les défis d'un environnement de la protection de la vie privée complexe et en évolution rapide, nos spécialistes de la recherche s'efforcent activement d'identifier les nouveaux enjeux et de les analyser afin de fournir des connaissances de base sur les domaines prioritaires. Le développement et la mise en commun des connaissances acquises dans le cadre de cette recherche constituent un volet primordial de la mission du Commissariat, qui consiste à promouvoir et à protéger le droit des personnes à la vie privée.

En partie en raison de cet environnement complexe et en évolution rapide, nous constatons que le travail

que nous accomplissons sur une question particulière est souvent pertinent pour nos mandats à la fois dans les secteurs privé et public. Le fait d'examiner les enjeux à partir de points de vue si différents a permis d'établir une base solide pour conseiller le Parlement, énoncer des positions de principe, mener des enquêtes et sensibiliser la population aux enjeux liés à la protection de la vie privée en général.

Les technologies et les techniques utilisées dans un secteur peuvent avoir différentes applications. Par exemple, les rapports que nous avons préparés sur la reconnaissance faciale et l'analyse prévisionnelle illustrent les enjeux qui chevauchent les mandats des secteurs public et privé.

6.7.1 Reconnaissance faciale

Une convergence de facteurs, comme la prolifération des caméras de surveillance, le stockage bon marché des données massives et les téléphones intelligents munis d'une caméra, ont fait en sorte que la reconnaissance faciale est devenue une technologie viable et de plus en plus fiable pour les gouvernements, la police et les intérêts commerciaux.

Le Commissariat a rédigé un rapport de recherche sur la technologie de reconnaissance faciale qui examine ces faits nouveaux. Le rapport conclut que les chercheurs et les décideurs ne font que commencer à rattraper leur retard dans la prise en compte des répercussions sociales de cette technologie.

6.7.2 Analyse prévisionnelle

L'analyse prévisionnelle est un autre domaine où les répercussions sociales n'ont pas encore fait l'objet d'études approfondies. Notre rapport de recherche examine le forage de données sur les clients à des fins de collecte d'indices sur les habitudes personnelles, les préférences et les habitudes d'achat, et il explique que ces techniques s'appliquent également au secteur public.

Notre examen de la question fait partie d'un effort continu pour comprendre la valeur des données massives pour les organisations, dans les secteurs privé et public, et pour réfléchir sur les répercussions sur la vie privée de ces nouvelles technologies.

6.7.3 Véhicules aériens sans pilote

Au cours de la dernière année, nous avons aussi commencé à examiner les répercussions sur la vie privée des véhicules aériens sans pilote (UAV), communément appelés « drones ». L'objectif était d'en apprendre davantage sur certaines utilisations actuelles et futures des véhicules aériens sans pilote à l'échelle du pays, par des organisations des secteurs public et privé, afin de comprendre la réglementation actuelle des vols de véhicules aériens sans pilote et de cerner toute préoccupation importante en matière de protection de la vie privée que pourrait susciter la prolifération de l'utilisation de ces véhicules au Canada.

À l'heure actuelle, l'utilisation de véhicules aériens sans pilote au Canada est encore assez limitée,

en raison des restrictions de la réglementation aérienne actuelle. Toutefois, le Commissariat est bien conscient que leur utilisation accrue pourrait entraîner d'importantes répercussions sur la vie privée selon les fins de leur utilisation, le contexte et le lieu de leur utilisation, ainsi que les types de technologies dont ils sont dotés. Par conséquent, le Commissariat continuera de surveiller la situation de près et, à l'avenir, s'il y a des changements dans l'utilisation de véhicules aériens sans pilote au Canada, nous nous attendons à prendre part à des discussions à ce sujet, et d'avoir l'occasion d'examiner des évaluations des facteurs relatifs à la vie privée.

6.8 ORIENTATION

L'élaboration d'une orientation pratique sur les principaux enjeux en matière de protection de la vie privée est un autre moyen que le Commissariat emploie pour s'acquitter de sa mission, qui consiste à promouvoir et à protéger le droit des personnes à la vie privée. En 2012-2013, nous avons produit deux nouvelles ressources d'orientation clés pour les organisations du secteur public, notamment des directives sur la façon de protéger les renseignements personnels dans les situations d'urgence et une trousse d'outils de gestion des atteintes à la vie privée pour les renseignements sur la santé.

6.8.1 Trousse d'urgence pour la protection des renseignements personnels

Le Commissariat a mis au point une trousse d'urgence pour la protection des renseignements personnels afin d'aider les organisations des secteurs public et privé assujetties aux lois fédérales sur la protection des renseignements personnels à améliorer le contenu et la rapidité des communications en cas d'urgence, tout en donnant aux gens l'assurance que leurs renseignements personnels seront traités de façon appropriée. Nous étions heureux d'élaborer ces directives en concertation avec plusieurs commissariats provinciaux et territoriaux de surveillance de la protection de la vie privée de tout le Canada.

La prise de mesures visant à prévoir la circulation de l'information en situation d'urgence fait partie intégrante d'une saine stratégie de gestion des risques pour toutes les organisations. Loin d'entraver la circulation de l'information, les lois sur la protection de la vie privée encouragent les organisations à bien se préparer de façon à permettre des interventions d'urgence qui respectent la vie privée, par exemple en élaborant des politiques et des protocoles d'échange de renseignements et en travaillant avec les représentants de Sécurité publique Canada qui ont aidé à faire connaître la trousse pendant la Semaine de la sécurité civile.

6.8.2 Trousse d'outils de gestion des atteintes à la vie privée pour les renseignements sur la santé

Au cours des dernières années, les représentants du Secrétariat du Conseil du Trésor du Canada

(SCT) ont coordonné un groupe de travail informel composé de membres provenant de plusieurs ministères fédéraux ayant des responsabilités relatives à l'exécution de programmes liés à la santé.

Les atteintes à la vie privée étant une préoccupation commune à ces ministères, on a demandé à un sous-groupe d'élaborer les principaux éléments d'une trousse d'outils de gestion des atteintes à la vie privée.

La trousse vise à donner aux institutions fédérales une compréhension commune de ce que constitue une atteinte à la vie privée et de la façon d'y répondre. Elle est fondée sur les Lignes directrices sur les atteintes à la vie privée du SCT, mais elle va plus loin en fournissant des outils et des directives sur le déroulement des opérations, du début à la fin — depuis l'arrêt de la fuite de données jusqu'aux leçons tirées de l'expérience.

Le Commissariat surveille le travail du sous-groupe, et nous attendons avec impatience l'achèvement du projet, ce qui contribuerait à assurer une approche uniforme et exhaustive de gestion des atteintes à la vie privée dans l'ensemble des ministères.

6.9 INTERVENTIONS DEVANT LES TRIBUNAUX

Aux termes de l'article 42 de la *Loi sur la protection des renseignements personnels*, la commissaire à la protection de la vie privée peut demander à comparaître devant la Cour fédérale lorsqu'une institution fédérale rejette une demande d'accès à des renseignements personnels déposée par une personne. Elle peut aussi à l'occasion faire l'objet de demandes de contrôle judiciaire.

Le Commissariat peut aussi demander à participer à titre d'intervenant dans d'autres affaires devant les cours ou autres tribunaux. Nous pouvons demander l'autorisation d'intervenir pour clarifier des questions liées à l'interprétation de certaines dispositions de la *Loi sur la protection des renseignements personnels*, ou pour donner à une cour ou à un tribunal notre point de vue sur d'autres questions juridiques ayant trait au droit à la vie privée ou à la protection des renseignements personnels.

Voici des résumés des affaires auxquelles nous avons participé en 2012-2013.

Conformément à l'esprit de notre mandat, nous ne publions pas le nom des plaignants. Toutefois, le numéro de dossier et le nom des institutions mises en cause sont fournis.

6.9.1 *X c. commissaire à la protection de la vie privée du Canada*

N° de dossier de la Cour : 2011 CF 1266;
confirmé en appel : 2012 CAF 229

Une personne a présenté une demande d'accès au Conseil de recherches en sciences humaines du Canada (CRSH), et s'est plainte par la suite au Commissariat que l'accès à ses renseignements personnels lui avait été refusé. Après enquête, nous avons déterminé que la plainte était **non fondée**.

Le plaignant sollicitait un contrôle judiciaire du rapport de conclusions du Commissariat. La demande a été rejetée avec dépens par la Cour fédérale. Le plaignant a interjeté appel auprès de la Cour d'appel fédérale, qui a également rejeté la demande avec dépens.

6.9.2 *X c. commissaire à la protection de la vie privée du Canada*

Nº de dossier de la Cour : 2013 CF 44

Le même plaignant a présenté une deuxième demande de contrôle judiciaire après notre enquête dans le cadre d'une autre plainte qui a donné lieu à une conclusion de plainte **non fondée**. La Cour fédérale a décrit la requête du demandeur comme n'ayant aucune chance de succès. Le Commissariat a recouvré ses dépens pour cette procédure.

6.9.3 *Commissaire à la protection de la vie privée du Canada c. Gendarmerie royale du Canada*

No de dossier de la Cour : T-1712-12

Une demande de nature judiciaire a été déposée par le Commissariat en vertu de l'article 42 de la *Loi sur la protection des renseignements personnels* à la suite d'une enquête sur une plainte relative à l'accès contre la Gendarmerie royale du Canada (GRC), qui a été jugée **fondée**. Par la suite, la GRC a accepté de diffuser les renseignements personnels demandés à l'origine par le plaignant, et nous avons abandonné la demande.

6.9.4 *X c. commissaire à la protection de la vie privée du Canada*

No de dossier de la Cour : T-125-13

Le demandeur a présenté une demande de contrôle judiciaire portant sur un rapport de conclusions du Commissariat, au sujet de l'enquête sur une plainte contre Ressources humaines et Développement des compétences Canada. Le demandeur cherche à contraindre le Commissariat à rouvrir la plainte. Ce dossier est actuellement devant la Cour fédérale.

6.9.5 *X c. Sa Majesté du Chef du Canada, et autres*

No de dossier de la Cour : CV-12-0716-00

Le demandeur dans ce dossier a intenté une poursuite contre 30 défendeurs représentant diverses entités fédérales, provinciales et municipales, ainsi que leurs employés. Au nombre des défendeurs figurent la commissaire à la protection de la vie privée et des employés du Commissariat.

En ce qui concerne les employés du Commissariat, les allégations du plaignant portent sur l'enquête effectuée par le Commissariat sur une plainte déposée par le plaignant contre Ressources humaines et Développement des compétences Canada. Le demandeur réclame des dommages-intérêts de tous les défendeurs. Ce dossier est actuellement devant la Cour supérieure de l'Ontario.

6.10 COMMUNICATION DE RENSEIGNEMENTS POUR DES RAISONS D'INTÉRÊT PUBLIC EN VERTU DE L'ALINÉA 8(2)*m*) DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

L'alinéa 8(2)*m*) 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;
- l'individu concerné en tirerait un avantage certain.

Les institutions qui ont l'intention de communiquer des renseignements pour des raisons d'intérêt public doivent en aviser le Commissariat par écrit, dans la mesure du possible avant que cette communication n'ait lieu ou tout de suite après.

Le Commissariat examine les communications prévues et peut exprimer son inquiétude concernant les communications proposées ou peut recommander que la personne dont les renseignements personnels sont communiqués soit avisée de la communication si l'institution ne l'a pas déjà fait. Si le ministère choisit de ne pas aviser la personne, la commissaire à la protection de la vie privée a le pouvoir de le faire.

Néanmoins, c'est au responsable de l'institution que revient la décision ultime de communiquer les renseignements d'une personne dans l'intérêt public. La commissaire n'a pas le pouvoir de s'opposer à cette décision.

Au cours de l'exercice 2012-2013, le Commissariat a examiné sa façon de traiter les avis des institutions qui avaient l'intention de communiquer des renseignements personnels dans l'intérêt public pour s'assurer qu'il y répond de manière appropriée. Certains ministères nous ont également consultés afin de passer en revue leurs documents de politique et de procédure sur le traitement des communications dans l'intérêt public.

En 2012-2013, nous avons traité 85 avis de communication en vertu de l'alinéa 8(2)*m*), par rapport à 107 au cours de l'exercice précédent. Voici quelques-uns des points saillants des avis de communication reçus par le Commissariat.

6.10.1 Gendarmerie royale du Canada

La Gendarmerie royale du Canada (GRC) a avisé le Commissariat de 19 communications de renseignements dans l'intérêt public en 2012-2013, soit le nombre le plus élevé de toutes les institutions. La plupart de ces communications concernaient des personnes qui devaient être libérées dans la communauté après avoir purgé une peine pour voies de fait ou agression sexuelle et qui présentaient un risque élevé de récidive.

6.10.2 Passeport Canada

Passeport Canada a communiqué 16 fois aux autorités sanitaires provinciales les coordonnées de personnes identifiées comme ayant occupé dans un avion commercial des places assises près d'une personne atteinte de tuberculose infectieuse latente. Dans les rapports annuels précédents, les communications de Passeport Canada étaient incluses avec celles du ministère des Affaires étrangères et du Commerce international.

6.10.3 Agence des services frontaliers du Canada

L'Agence des services frontaliers du Canada (ASFC) a avisé le Commissariat de 11 communications de renseignements dans l'intérêt public qui concernaient en grande partie le retrait d'individus de la liste des « personnes recherchées par l'ASFC ».

6.10.4 Service correctionnel du Canada

Le Service correctionnel du Canada a effectué 11 communications, soit pour informer les victimes avant le transfert d'un détenu à un autre pénitencier, soit pour fournir aux membres de la famille un rapport d'enquête sur la mort d'un détenu.

6.10.5 Ressources humaines et Développement des compétences Canada

Ressources humaines et Développement des compétences Canada a avisé le Commissariat de neuf communications de renseignements dans l'intérêt public au cours de l'exercice financier. Bon nombre de ces communications ont été effectuées aux services de police pour retrouver une personne disparue ou pour aviser les plus proches parents lorsqu'une personne a menacé de se blesser ou de blesser gravement d'autres personnes.

Les autres communications de renseignements dans l'intérêt public étaient attribuables au ministère de la Défense nationale (5), à la Commission de l'immigration et du statut de réfugié du Canada (3), à Transports Canada (3), au ministère des Affaires étrangères et du Commerce international (2), à Sécurité publique Canada (2). Une communication de renseignements dans l'intérêt public a été effectuée par chacune des institutions suivantes : Agence du revenu du Canada, Tribunal canadien des droits de la personne, Exportation et développement Canada et Affaires autochtones et Développement du Nord Canada.

7.0 L'année à venir

À quelles nouveautés concrètes le Commissariat peut-il s'attendre au cours des 12 prochains mois? Que pouvons-nous prévoir clairement comme étant la prochaine étape du débat canadien sur la protection des renseignements personnels et la sphère personnelle? Voici quelques questions que nous pouvons voir émerger à l'horizon.

7.1 SIGNALEMENT OBLIGATOIRE DES ATTEINTES À LA VIE PRIVÉE

Les Canadiennes et les Canadiens ont le droit d'en savoir davantage sur la façon dont leurs renseignements sont utilisés et communiqués par le gouvernement fédéral.

Bien que les intervenants du secteur privé répondent proactivement aux demandes en vue d'une plus grande transparence à cet égard, il reste encore beaucoup à faire du côté des institutions gouvernementales du Canada.

De même, les exigences relatives au signalement des atteintes à la vie privée dans les secteurs public et privé semblent être à la base de l'amélioration des approches en matière de cybersécurité à l'échelle du système.

Le Commissariat s'emploie activement à discuter des exigences relatives au signalement obligatoire des atteintes à la vie privée avec d'autres organisations fédérales œuvrant dans le domaine de la cybersécurité, notamment le Secrétariat du Conseil du Trésor du Canada, Sécurité publique Canada, la Gendarmerie royale du Canada et le Bureau de la concurrence Canada. Nous espérons que le signalement des atteintes à la vie privée devienne obligatoire pour l'ensemble des organisations fédérales dans un avenir rapproché.

7.2 MISE À JOUR DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

La logique voulant que le gouvernement soit assujetti à une norme équivalente ou même plus élevée que le secteur privé devrait trouver écho chez de nombreux Canadiens. Le plus récent rapport annuel du greffier du Conseil privé invite les organisations fédérales à se montrer à la hauteur du dynamisme manifesté par le secteur privé et à s'astreindre à respecter les mêmes normes et attentes que ce dernier. Cela devrait également s'appliquer au traitement des renseignements personnels des Canadiennes et Canadiens.

Au cours des dernières années, il y a eu un débat ouvert et approfondi sur le degré de soin attendu des citoyens de la part du gouvernement fédéral en ce qui concerne le traitement, la communication et la protection des renseignements sensibles.

Les atteintes à la sécurité des renseignements personnels au sein des organisations gouvernementales, le débat ouvert sur le mérite relatif de diverses mesures de surveillance technique, les questions sur la façon dont les tribunaux canadiens perçoivent les limites et les mesures de protection appropriées visant les renseignements personnels et les communications privées ont tous contribué à cette discussion.

Au cœur de ces questions se trouve la législation régissant la protection des renseignements personnels dans le secteur public, qui n'a pas fait l'objet d'une mise à jour approfondie en trois décennies, lesquelles ont été marquées par des changements technologiques considérables et l'échange accru de renseignements outre-frontière.

Il est approprié, opportun et sain que les Canadiennes et Canadiens tiennent un débat sur cette question.

7.3 SURVEILLANCE, EN LIGNE ET HORS LIGNE

Nous pouvons nous attendre à ce que se poursuivent les débats passionnés sur le programme de sécurité nationale du gouvernement et le droit à la vie privée dont nous bénéficions en tant que citoyens. Les médias poseront des questions, les universitaires mèneront des études et engageront des débats, le gouvernement défendra ses positions et les parlementaires entreprendront une procédure d'examen — tout cela dans le but d'améliorer notre société ouverte et démocratique.

Cependant, compte tenu du nombre sans précédent de nouveaux types de menaces et de l'accroissement rapide de la capacité de surveillance, nos mesures traditionnelles de protection de la vie privée doivent maintenant aussi faire l'objet d'un débat sérieux.

Le Canada doit rajuster les tensions entre la protection de la vie privée et la sécurité. Le débat entourant l'atteinte de cet objectif ne peut se tenir que si la discussion est engagée à tous les niveaux de notre société. Il s'agit d'une discussion ouverte que le Commissariat accueille favorablement et à laquelle il espère contribuer au moyen de recherches, de discours, de rapports et de travail à l'échelon international.

7.4 CONFUSION ENTRE LES RESPONSABILITÉS DU COMMISSARIAT ET CELLES DES MINISTÈRES

Nous avons constaté que les ministères et organismes fédéraux « consultent » davantage le Commissariat puis laissent entendre publiquement par la suite que ce seul geste a permis de régler ou d'éliminer tous les risques liés à la vie privée. Or, bien que nous fassions de notre mieux pour contribuer à protéger le droit à la vie privée des Canadiennes et Canadiens, le Commissariat n'a pas le pouvoir de contraindre la mise en œuvre des recommandations qu'il a formulées au sujet d'évaluations des facteurs relatifs à la vie privée (EFVP).

La responsabilité et la reddition de comptes en ce qui concerne les risques pour la vie privée incombent au bout du compte à l'institution fédérale. Lorsque les Bureaux d'accès à l'information et de protection des renseignements personnels des organismes et ministères se fient trop au Commissariat, ils ne développent pas leur propre capacité à élaborer des EFVP et à aborder les enjeux liés à la protection de la vie privée.

Nous sommes en train d'accroître nos activités de sensibilisation afin de fournir une orientation aux représentants de ces bureaux, afin qu'on puisse de plus en plus compter sur eux au sein de leurs institutions pour apporter une expertise bien nécessaire et utile en matière de protection de la vie privée.

7.5 AVIS INSUFFISANT

Au cours de la prochaine année, nous suivrons de près une tendance croissante qui menace le respect des besoins des Canadiennes et Canadiens en matière d'information. Dans plusieurs des EFVP que nous avons reçues cette année, le Commissariat a constaté que des organisations décident de ne pas apposer d'affiches indiquant publiquement une surveillance vidéo. On a informé le Commissariat que, dans les régions frontalières, il y a un prétendu risque d'« encombrement d'affiches », et que la disposition physique de certains espaces fait en sorte qu'il est difficile ou inesthétique d'installer des affiches bien en vue.

Certaines institutions ont opté pour d'autres formes d'avis public, comme un plan de communications publiques, au lieu d'affiches. Nous suivrons cette tendance de près.

7.6 MACRO-PROJETS, MICRO-EXAMEN

Le plan d'action *Par-delà la frontière* présente des défis uniques pour les EFVP. Le passage à un modèle de périmètre pour la sécurité frontalière signifie que de nombreuses EFVP ne tiennent pas compte des liens innombrables qui existent entre des programmes et des activités qui sont parfois nombreux et distincts.

Par conséquent, plusieurs EFVP que nous avons reçues cette année ne faisaient pas état d'une approche suffisamment globale pour permettre une analyse convaincante de la façon dont les changements découlant du plan d'action *Par delà la frontière* pourraient avoir des répercussions sur la protection de la vie privée dans un contexte plus large. Compte tenu du fait que davantage d'EFVP liées à cette initiative sont prévues au cours de l'année à venir, nous avons tenté de communiquer ce problème à l'échelle du gouvernement, y compris en offrant une séance pendant notre atelier annuel sur la manière dont les ministères peuvent collaborer à la réalisation d'une EFVP interministérielle dans l'espoir que cela favorisera une analyse plus globale et intégrée.

7.7 TOUT COMMUNIQUER

La collaboration transfrontalière entre les gouvernements donne lieu à un échange de renseignements de plus en plus grand entre les frontières. Au cours de l'année, nous avons reçu plusieurs EFVP portant sur des initiatives visant à faciliter l'échange systématique de renseignements entre les gouvernements fédéraux canadien et américain. Dans le passé, de tels échanges de renseignements étaient examinés avec soin au cas par cas.

Au cours de la dernière année, le Commissariat a toutefois remarqué une tendance caractérisée par la systématisation et l'élargissement considérable de ces processus. On s'attend à ce que cette tendance se poursuive tout au long des prochaines étapes du plan d'action *Par-delà la frontière* et des diverses initiatives de sécurité du périmètre.

Bien que le Canada et les États-Unis soient similaires sous de nombreux aspects, les deux pays ont des régimes de protection de la vie privée très différents. Même si le Commissariat s'est efforcé de cerner les principaux risques pour la vie privée lors du processus d'examen, il nous est impossible de prévoir où il pourrait y avoir des écarts entre les deux administrations lorsqu'il est question de projets d'une envergure et d'une complexité aussi grandes.

7.8 REGROUPEMENT DES SERVICES ET IMPARTITION

La recherche de gains d'efficience dans l'ensemble des institutions fédérales se poursuit, et nous continuerons de surveiller de près les initiatives afin que la protection de la vie privée ne soit pas laissée en arriere-plan. Le passage au regroupement ou au partage de services a été fait de manière officielle par la création de Services partagés Canada, qui est axé sur la gestion de l'infrastructure des technologies de l'information du gouvernement, et aussi de façon moins officielle par des activités comme le regroupement des systèmes de ressources humaines et de gestion financière des institutions de petite et de moyenne tailles.

Nous avons également constaté que le gouvernement fédéral cherche à tirer parti des capacités et des infrastructures existantes à de nouvelles fins :

- au sein du gouvernement, notamment l'utilisation de systèmes existants pour le stockage de nouvelles données biométriques;
- avec le secteur privé, notamment le stockage des dossiers et les fonctions liées aux ressources humaines.

Compte tenu de la situation financière actuelle et des pressions qui s'exercent en vue de la rationnalisation de la prestation des programmes, nous prévoyons que cette tendance se poursuivra. Le Commissariat continuera d'offrir des conseils sur la protection des renseignements personnels aux institutions à mesure qu'elles s'engagent dans cette voie.

7.9 ENQUÊTES DE SÉCURITÉ AU GOUVERNEMENT FÉDÉRAL

En ce qui concerne les enquêtes de sécurité, des changements devraient se produire au cours de la prochaine année. Pendant l'année qui vient de s'écouler, le Commissariat a examiné des EFVP qui soulevaient des préoccupations quant à la façon dont ces enquêtes sont effectuées par les ministères et les organismes, mettant ainsi en évidence la nécessité de se pencher sur la question.

Nous avons découvert que les pratiques varient beaucoup d'une organisation à une autre, car la Norme sur la sécurité du personnel du SCT laisse de nombreux aspects à la discrétion des agents de sécurité du ministère.

Au sein du gouvernement fédéral, il y a un recours accru à des vérifications du crédit et un plus grand intérêt à recevoir des données de non-condamnation de la Gendarmerie royale du Canada (GRC), plutôt que de s'en tenir aux renseignements sur les casiers judiciaires. De plus, un nombre croissant d'institutions demandent l'autorisation d'employer des méthodes de contrôle approfondi, comme l'examen polygraphique et des questionnaires de contrôle possiblement attentatoires, comme celui

qui a été retiré par l'Agence des services frontaliers du Canada à la suite d'une réaction défavorable du public (tel qu'il est expliqué au chapitre 6).

Dans ce contexte, le SCT révise actuellement la Norme sur la sécurité du personnel. Le Commissariat collaborera étroitement avec les responsables du SCT au moment de l'élaboration de la nouvelle norme afin d'assurer un dialogue productif quant aux risques pour la vie privée associés aux changements potentiels.

On nous a assurés qu'une EFVP sur la nouvelle norme sera effectuée par le SCT, et nous nous attendons à ce que les institutions qui mettent en œuvre de nouvelles pratiques en matière d'enquêtes de sécurité mènent leurs propres évaluations.

Bien qu'il soit manifestement nécessaire de veiller à ce que la fonction publique fédérale soit composée de personnes qui sont dignes de confiance, fiables et loyales à l'égard de l'intérêt national, nous devons veiller à ce que les mesures d'enquête de sécurité envahissantes qui sont mises en œuvre s'avèrent nécessaires et efficaces pour le maintien de ces qualités.

7.10 AUTRES DOMAINES

Le présent rapport décrit plus haut le projet de modernisation visant à rationaliser notre processus d'enquête (chapitre 6). Au cours de l'année à venir, nous mettrons en œuvre ses recommandations. Bien que des gains d'efficience aient déjà été réalisés dans certains domaines, le plein effet de quelques-unes des mesures pourrait prendre plus d'un an à se faire ressentir.

Nous continuons d'agrandir notre laboratoire d'essai à la fine pointe de la technologie afin de renforcer notre capacité de soutien technologique à l'appui des nouvelles enquêtes.

Annexe 1

DÉFINITIONS

Types de plaintes

1. Accès

Accès — Tous les renseignements personnels n'ont pas 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 les renseignements.

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

Langue — Les renseignements personnels n'ont pas été fournis dans la langue officielle demandée.

Frais — Des frais ont été exigés pour répondre à la demande de renseignements en vertu de la *Loi sur la protection des renseignements personnels*; aucun frais n'est actuellement prévu pour l'obtention de renseignements personnels.

Répertoire — *Info Source* (un 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 décrit pas de façon adéquate le fonds de renseignements personnels d'une institution.

2. Protection des renseignements personnels

Collecte — Une institution a recueilli des renseignements personnels qui ne sont pas nécessaires à l'exploitation d'un de ses programmes ou à l'une de ses activités, les renseignements personnels n'ont pas été recueillis directement auprès de la personne concernée, ou la personne n'a pas été informée des fins pour lesquelles les renseignements personnels ont été recueillis.

Conservation et retrait — Des renseignements personnels ne sont pas conservés selon les calendriers de conservation et de retrait approuvés par les Archives nationales et publiés dans *Info Source* : ils sont 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 application d'une mesure administrative, à moins que la personne ait consenti à leur retrait.

Utilisation et communication — Des renseignements sont utilisés ou communiqués sans le consentement de la personne concernée et ne satisfont pas à l'un des critères d'utilisation ou de communication permise sans consentement énoncés aux articles 7 et 8 de la *Loi*.

3. Délais

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

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

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

Conclusions et autres décisions 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*. Cette catégorie comprend les conclusions auparavant désignées « fondées et résolues », c'est-à-dire où les allégations étaient corroborées par l'enquête et l'institution fédérale acceptait de prendre des mesures correctives afin de remédier à la situation.

Non fondée : L'enquête n'a pas permis de déceler les éléments de preuve qui suffisent à 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*.

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.

2. Autres décisions

Réglée rapidement : S'applique aux cas où l'affaire est réglée avant même qu'une enquête officielle ne soit entamée. Par exemple, si une personne dépose une plainte dont le sujet a déjà fait l'objet d'une enquête par le Commissariat et a été considéré conforme à la *Loi sur la protection des renseignements personnels*, nous expliquons la situation à cette personne. Il nous arrive également de recevoir des plaintes pour lesquelles une enquête officielle aurait pu avoir des conséquences défavorables pour la personne. En pareil cas, nous expliquons en détail la situation au plaignant. Si ce dernier décide de ne pas poursuivre l'affaire, le dossier est fermé et la plainte est considérée comme étant « réglée rapidement ».

Réglée en cours d'enquête : Le Commissariat a participé à la négociation d'une solution satisfaisant toutes les parties dans le cadre de l'enquête, mais aucune conclusion n'a été rendue.

Abandonnée : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons. Par exemple, le plaignant pourrait ne plus vouloir donner suite à l'affaire, ou ne plus être joignable pour fournir des renseignements supplémentaires essentiels pour arriver à une conclusion.

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

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 officielle. 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 officielle :

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 2

TABLEAUX CONCERNANT LES PLAINTES EN VERTU DE LA LPRP POUR LE RAPPORT ANNUEL DE 2012-2013

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

	Règlement rapide		Enquêtes		Nombre total	Pourcentage total
Type de plainte	**Nombre**	**Pourcentage**	**Nombre**	**Pourcentage**		
Accès						
Accès	92	4,05 %	280	12,32 %	372	**16,37 %**
Correction – Avis	5	0,22 %	0	0,00 %	5	**0,22 %**
Refus de donner accès	1	0,04 %	0	0,00 %	1	**0,04 %**
Délais						
Délais	108	4,75 %	305	13,42 %	413	**18,17 %**
Avis de prorogation de délai	6	0,26 %	12	0,53 %	18	**0,79 %**
Correction – délai	3	0,13 %	3	0,13 %	6	**0,26 %**
Protection des renseignements personnels						
Utilisation et divulgation	82	3,61 %	1334	58,69 %	1416	**62,30 %**
Collecte	12	0,53 %	16	0,70 %	28	**1,23 %**
Conservation et élimination	3	0,13 %	7	0,31 %	10	**0,44 %**
Politique	2	0,09 %	0	0,00 %	2	**0,09 %**
Plainte déposée par la commissaire	0	0,00 %	2	0,09 %	2	**0,09 %**
Total	**314**	**13,81 %**	**1959**	**86,19 %**	**2273**	**100,00 %**

Dix institutions ayant fait l'objet du plus grand nombre de plaintes en vertu de la LPRP acceptées

Mis en cause	Accès		Délai		Protection des renseignements personnels		Plainte déposée par la commissaire	Total
	Règlement rapide	Enquête	Règlement rapide	Enquête	Règlement rapide	Enquête	Enquête	
Ressources humaines et Développement des compétences Canada	2	5	1	4	16	1 001	1	**1 030**
Service correctionnel du Canada	24	66	47	91	16	40	0	**284**
Ministère de la Justice Canada	1	17	0	5	2	162	1	**188**
Gendarmerie royale du Canada	20	38	6	90	11	17	0	**182**
Ministère de la Défense nationale	8	13	19	33	1	16	0	**90**
Agence des services frontaliers du Canada	7	21	6	12	2	40	0	**88**
Agence du revenu du Canada	7	32	7	14	4	12	0	**76**
Anciens Combattants Canada	1	2	7	28	4	14	0	**56**
Agence canadienne d'inspection des aliments	2	5	10	14	0	2	0	**33**
Transports Canada	0	8	2	7	3	7	0	**27**
Total	**72**	**207**	**105**	**298**	**59**	**1 311**	**2**	**2 054**

Dix institutions ayant fait l'objet du plus grand nombre de plaintes en vertu de la LPRP acceptées en 2012-2013 et nombre de plaintes déposées au cours des différents exercices

Organisation	2009-2010	2010-2011	2011-2012	2012-2013
Ressources humaines et Développement des compétences Canada	20	25	26	1 030
Service correctionnel du Canada	290	276	326	284
Ministère de la Justice Canada	11	9	9	188
Gendarmerie royale du Canada	60	75	117	182
Ministère de la Défense nationale	47	65	115	90
Agence des services frontaliers du Canada	26	29	55	88
Agence du revenu du Canada	49	53	65	76
Anciens Combattants Canada	2	15	39	56
Agence canadienne d'inspection des aliments	0	8	3	33
Transports Canada	8	14	6	27
Grand Total	**513**	**569**	**761**	**2 054**

Plaintes en vertu de la LPRP acceptées, par institution

Mis en cause	Règlement rapide	Enquête	Total
Affaires autochtones et Développement du Nord Canada	3	15	18
Agriculture et Agroalimentaire Canada	8	1	9
Agence des services frontaliers du Canada	15	73	88
Agence de développement économique du Canada pour les régions du Québec	0	2	2
Société canadienne des postes	14	7	21
Agence du revenu du Canada	18	58	76
École de la fonction publique du Canada	0	1	1
Société Radio Canada	1	0	1
Agence canadienne d'inspection des aliments	12	21	33
Patrimoine canadien	0	1	1
Commission canadienne des droits de la personne	1	1	2

Plaintes en vertu de la LPRP acceptées, par institution (suite)

Mis en cause	Règlement rapide	Enquête	Total
Tribunal canadien des droits de la personne	0	2	2
Musée canadien des civilisations	0	1	1
Conseil de la radiodiffusion et des télécommunications canadiennes	1	0	1
Service canadien du renseignement de sécurité	3	16	19
Citoyenneté et Immigration Canada	11	6	17
Service correctionnel du Canada	87	197	284
Élections Canada	1	1	2
Environnement Canada	1	1	2
Pêches et Océans Canada	1	6	7
Affaires étrangères et Commerce international Canada	2	5	7
Santé Canada	1	5	6
Ressources humaines et Développement des compétences Canada	19	1011	1030
Commission de l'immigration et du statut de réfugié	3	0	3
Résolution des questions des pensionnats indiens Canada	1	0	1
Industrie Canada	2	1	3
Ministère de la Justice Canada	3	185	188
Bibliothèque et Archives Canada	1	0	1
Commission d'examen des plaintes concernant la police militaire	0	3	3
Ministère de la Défense nationale	28	62	90
Ressources naturelles Canada	0	1	1
Conseil de recherches en sciences naturelles et en génie	0	1	1
Bureau de l'infrastructure	0	1	1
Commissariat aux langues officielles	0	1	1
Bureau de l'enquêteur correctionnel	1	1	2
Commissariat à l'information du Canada	1	1	2
Agence Parcs Canada	1	0	1
Commission nationale des libérations conditionnelles	0	1	1
Passeport Canada	6	3	9

Plaintes en vertu de la LPRP acceptées, par institution (suite)

Mis en cause	Règlement rapide	Enquête	Total
Bureau du Conseil privé	0	2	2
Agence de la santé publique du Canada	3	4	7
Service des poursuites pénales du Canada	0	2	2
Sécurité publique Canada	1	2	3
Commissariat à l'intégrité du secteur public du Canada	0	1	1
Commission de la fonction publique du Canada	0	3	3
Tribunal de la dotation de la fonction publique	1	0	1
Travaux publics et Services gouvernementaux Canada	3	17	20
Monnaie royale canadienne	0	2	2
Gendarmerie royale du Canada	37	145	182
Comité d'examen externe de la Gendarmerie royale du Canada	0	1	1
Service Canada	2	1	3
Services partagés Canada	2	0	2
Conseil de recherches en sciences humaines	0	1	1
Statistique Canada	1	17	18
Transports Canada	5	22	27
Bureau de la sécurité des transports du Canada	0	1	1
Secrétariat du Conseil du Trésor du Canada	1	1	2
Anciens Combattants Canada	12	44	56
Tribunal des anciens combattants (révision et appel)	0	1	1
Total	**314**	**1 959**	**2 273**

Plaintes en vertu de la LPRP acceptées par province ou territoire

	Règlement rapide		Enquête		Nombre total	Pourcentage total
Province ou territoire	**Nombre**	**Pourcentage**	**Nombre**	**Pourcentage**		
Alberta	27	1,19 %	134	5,90 %	161	7,08 %
Colombie-Britannique	64	2,82 %	197	8,67 %	261	11,48 %
Manitoba	18	0,79 %	33	1,45 %	51	2,24 %
Nouveau-Brunswick	9	0,40 %	31	1,36 %	40	1,76 %
Terre-Neuve-et-Labrador	1	0,04 %	15	0,66 %	16	0,70 %
Territoires du Nord-Ouest	0	0,00 %	2	0,09 %	2	0,09 %
Non précisé	1	0,04 %	3	0,13 %	4	0,18 %
Nouvelle-Écosse	18	0,79 %	56	2,46 %	74	3,26 %
Ontario	129	5,68 %	1 260	55,43 %	1 389	61,11 %
Autre (pas États-Unis)	1	0,04 %	6	0,26 %	7	0,31 %
Île-du-Prince-Édouard	1	0,04 %	7	0,31 %	8	0,35 %
Québec	33	1,45 %	164	7,22 %	197	8,67 %
Saskatchewan	8	0,35 %	23	1,01 %	31	1,36 %
États-Unis	4	0,18 %	1	0,04 %	5	0,22 %
(vide)	0	0,00 %	27	1,19 %	27	1,19 %
Total	**314**	**13,81 %**	**1 959**	**86,19 %**	**2 273**	**100,00 %**

Décision rendue quant aux plaintes en vertu de la LPRP, par type de plainte

Type de plainte	Fondées	Fondées résolues	Non fondées	Résolues	Abandonnées	RR-Résolues	Pas de la compétence du CPVP	Réglées	Total
Accès									
Accès	24	46	117	18	21	101	4	23	354
Correction – Avis	0	0	0	0	0	6	0	0	6
Langue	0	0	0	0	2	0	0	0	2
Frais	0	0	0	0	1	0	0	0	1
Délais									
Délais	197	0	12	2	13	108	0	2	334
Avis de prorogation de délai	3	0	3	0	1	6	0	0	13
Correction – Délai	2	0	0	0	0	0	0	0	2
Protection des renseignements personnels									
Utilisation et divulgation	49	1	25	1	18	64	1	7	166
Collecte	1	0	6	0	4	10	0	1	22
Conservation et élimination	0	0	3	1	0	2	0	0	6
Politique	0	0	0	0	0	2	0	0	2
Total	**276**	**47**	**166**	**22**	**60**	**299**	**5**	**33**	**908**

Décisions rendues quant aux plaintes en vertu de la LPRP relatives aux délais, par institution

Mis en cause	Fondées	Non fondées	Résolues	Abandonnées	RR-Résolues	Réglées	Total
Affaires autochtones et Développement du Nord Canada	0	0	0	0	1	0	1
Agence des services frontaliers du Canada	8	2	0	0	8	0	18
Société canadienne des postes	0	1	0	0	0	0	1
Agence du revenu du Canada	16	1	0	0	4	0	21
Agence canadienne d'inspection des aliments	12	0	0	0	10	0	22
Citoyenneté et Immigration Canada	2	0	0	1	3	0	6
Service correctionnel du Canada	65	3	1	1	34	0	104
Pêches et Océans Canada	2	1	0	0	0	0	3
Affaires étrangères et Commerce international Canada	1	0	0	0	2	0	3
Santé Canada	0	0	0	0	1	0	1
Ressources humaines et Développement des compétences Canada	4	0	0	1	1	0	6
Ministère de la Défense nationale	39	1	1	10	27	0	78
Ressources naturelles Canada	1	0	0	0	0	0	1
Agence Parcs Canada	0	0	0	0	1	0	1
Agence de la santé publique du Canada	0	0	0	0	2	0	2
Service des poursuites pénales du Canada	1	1	0	0	0	0	2
Travaux publics et Services gouvernementaux Canada	5	0	0	0	1	0	6
Monnaie royale canadienne	0	1	0	0	0	0	1
Gendarmerie royale du Canada	32	2	0	1	7	2	44
Statistique Canada	0	2	0	0	0	0	2
Transports Canada	4	0	0	0	3	0	7
Secrétariat du Conseil du Trésor du Canada	0	0	0	0	1	0	1
Anciens Combattants Canada	10	0	0	0	7	0	17
Service Canada	0	0	0	0	1	0	1
Total	**202**	**15**	**2**	**14**	**114**	**2**	**349**

Décisions rendues quant aux plaintes en vertu de la LPRP relatives à l'accès à l'information et à la protection des renseignements personnels, par institution

Mis en cause	Fondées	Fondées résolues	Non fondées résolues	Résolues	Abandonnées	RR-Résolues	Pas de la compétence du CPVP	Réglées	Total
Affaires autochtones et Développement du Nord Canada	1	0	1	0	0	2	0	0	4
Agriculture et Agroalimentaire Canada	0	0	1	0	0	8	0	0	9
Agence des services frontaliers du Canada	3	2	11	3	4	14	0	2	39
Société canadienne des postes	1	2	2	0	2	17	0	2	26
Agence du revenu du Canada	4	5	20	2	1	11	0	3	46
Société Radio-Canada	0	0	1	0	0	1	0	0	2
Agence canadienne d'inspection des aliments	1	0	1	0	0	2	0	0	4
Comité des griefs des Forces canadiennes	0	1	0	0	0	0	0	0	1
Commission canadienne des droits de la personne	0	2	0	0	0	1	0	0	3
Tribunal canadien des droits de la personne	0	0	1	0	0	0	0	1	2
Conseil de la radiodiffusion et des télécommunications canadiennes	0	0	0	0	0	1	0	0	1
Service canadien du renseignement de sécurité	0	0	18	0	1	3	0	0	22
Agence spatiale canadienne	0	0	3	0	0	0	0	0	3
Citoyenneté et Immigration Canada	1	6	5	0	0	5	0	1	18
Service correctionnel du Canada	49	10	38	7	11	44	1	4	164
Élections Canada	0	0	0	0	0	1	0	0	1
Environnement Canada	0	1	0	0	0	1	0	0	2
Pêches et Océans Canada	0	0	2	1	0	1	0	0	4
Affaires étrangères et Commerce international Canada	0	0	1	0	0	0	0	0	1
Santé Canada	0	0	1	0	0	0	0	1	2
Ressources humaines et Développement des compétences Canada	1	3	2	0	1	8	0	3	18
Commission de l'immigration et du statut de réfugié	0	0	1	0	1	0	0	0	2
Résolution des questions des pensionnats indiens Canada	0	0	0	0	0	1	0	0	1
Industrie Canada	0	1	1	0	0	2	0	1	5

Décisions rendues quant aux plaintes en vertu de la LPRP relatives à l'accès à l'information et à la protection des renseignements personnels, par institution (suite)

Mis en cause	Fondées	Fondées résolues	Non fondées résolues	Résolues	Abandonnéees	RR-Résolues	Pas de la compétence du CPVP	Réglées	Total
Ministère de la Justice Canada	0	1	0	0	1	3	0	1	6
Bibliothèque et Archives Canada	0	0	0	0	0	0	0	1	1
Commission d'examen des plaintes concernant la police militaire	0	0	0	0	1	0	0	0	1
Ministère de la Défense nationale	4	3	8	2	1	11	0	5	34
Musée des beaux-arts du Canada	0	0	0	0	1	0	0	0	1
Conseil national de recherches du Canada	0	1	1	0	0	0	0	0	2
Ressources naturelles Canada	0	1	1	0	1	0	0	0	3
Bureau de l'enquêteur correctionnel	0	0	0	0	0	1	0	0	1
Commissariat à l'information du Canada	0	0	0	0	0	1	0	0	1
Agence Parcs Canada	1	0	0	0	0	0	0	0	1
Commission nationale des libérations conditionnelles	0	0	0	0	1	0	3	0	4
Passeport Canada	0	0	1	0	0	3	0	0	4
Agence de la santé publique du Canada	0	1	0	0	5	1	0	0	7
Service des poursuites pénales du Canada	0	0	1	0	0	0	0	0	1
Sécurité publique Canada	0	0	1	0	0	1	0	0	2
Tribunal de la dotation de la fonction publique	0	0	0	0	0	1	0	0	1
Travaux publics et Services gouvernementaux Canada	0	1	6	1	0	2	0	0	10
Gendarmerie royale du Canada	6	4	19	4	10	28	0	6	77
Services partagés Canada	0	0	0	0	0	1	0	0	1
Statistique Canada	1	1	0	0	0	1	0	0	3
Transports Canada	0	0	0	0	1	3	0	0	4
Secrétariat du Conseil du Trésor du Canada	0	0	0	0	0	1	0	0	1
Anciens Combattants Canada	1	0	3	0	2	4	1	0	11
Tribunal des anciens combattants (révision et appel)	0	0	0	0	1	0	0	0	1
VIA Rail Canada	0	1	0	0	0	0	0	0	1
Total	**74**	**47**	**151**	**20**	**46**	**185**	**5**	**31**	**559**

Délais de traitement des plaintes en vertu de la LPRP – Plaintes réglées rapidement, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen (mois)
Accès		
Accès	101	2,12
Correction – Avis	6	1,26
Délais		
Délais	108	2,42
Avis de prorogation de délai	6	0,20
Protection des renseignements personnels		
Utilisation et divulgation	64	2,48
Collecte	10	2,12
Politique	2	2,38
Conservation et élimination	2	2,23
Total	**299**	**2,25**

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

Complaint Type	Nombre	Délai de traitement moyen (mois)
Accès		
Accès	264	11,82
Langue	2	21,61
Frais	1	19,11
Délais		
Délais	228	4,46
Avis de prorogation de délai	7	4,99
Correction – délai	2	6,41
Protection des renseignements personnels		
Utilisation et divulgation	111	10,69
Collecte	14	8,88
Conservation et élimination	4	15,43
Total	**633**	**8,88**

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

Décision rendue	Nombre	Average Treatment Time (Months)
Plaintes officielles		
Fondée	276	7,10
Non fondée	166	10,80
Abandonnée	60	9,07
Fondée et résolue	47	14,51
Réglée	33	8,68
Résolue	22	10,62
RR-Non fructueux	17	3,23
RR-Non approprié	7	4,11
Absence de compétence	5	7,97
RR-Résolue	**299**	**2,25**
Total	**932**	**6,75**

Incidents liés à la LPRP, par institution

Mis en cause	Incident
Agence du revenu du Canada	22
Service correctionnel du Canada	17
Ressources humaines et Développement des compétences Canada	11
Affaires étrangères et Commerce international Canada	10
Citoyenneté et Immigration Canada	5
Anciens Combattants Canada	5
Société canadienne des postes	4
Statistique Canada	4
Ministère de la Défense nationale	3
Gendarmerie royale du Canada	2
Passeport Canada	2
Services partagés Canada	2
Pêches et Océans Canada	2
Exportation et développement Canada	2
Santé Canada	2
Affaires autochtones et Développement du Nord Canada	2
Administration canadienne de la sûreté du transport aérien	2
Élections Canada	1
Agence canadienne d'inspection des aliments	1
La Fondation Pierre-Elliott-Trudeau	1
Bibliothèque et Archives Canada	1
Conseil de la radiodiffusion et des télécommunications canadiennes	1
Commission canadienne des droits de la personne	1
Environnement Canada	1
Centre d'analyse des opérations et déclarations financières du Canada	1
Transports Canada	1
Service des poursuites pénales du Canada	1
Ministère de la Justice Canada	1
Travaux publics et Services gouvernementaux Canada	1
Total	**109**