Rapport annuel au Parlement 2013-14

TRANSPARENCE ET VIE PRIVÉE À L'ÈRE NUMÉRIQUE

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

Commissariat
à la protection de
la vie privée du Canada

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

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

Nº de catalogue : IP50-2014F-PDF
1913-7559

Cette publication se trouve également sur le site **www.priv.gc.ca**

Suivez-nous sur Twitter : @PriveePrivacy

Commissaire à la protection de la vie privée du Canada

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

Privacy Commissioner of Canada

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

Octobre 2014

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 2013 au 31 mars 2014.

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

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

Original signé par

Daniel Therrien

Commissaire à la protection de la vie privée du Canada

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

Privacy Commissioner of Canada

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

Octobre 2014

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

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels* pour la période du 1er avril 2013 au 31 mars 2014.

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

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

Original signé par

Daniel Therrien

Table des matières

1 Message du commissaire

Le droit à la vie privée fait partie de nos libertés et droits fondamentaux en tant que Canadiens, et dans le contexte d'une capacité technologique en évolution constante qui permet de recueillir et d'analyser les renseignements personnels, nous devons protéger ce droit en faisant preuve d'un engagement et d'une vigilance constants.

J'ai été nommé commissaire à la protection de la vie privée après la fin de la période 2013-2014 visée par le présent rapport annuel concernant la *Loi sur la protection des renseignements personnels*. Je n'étais donc pas à la tête de l'organisation durant l'année qui vient de s'écouler où la protection de la vie privée a gagné en importance, et pour cause! Jamais, dans l'histoire de l'humanité, les renseignements personnels n'ont été aussi accessibles qu'aujourd'hui et, par conséquent, jamais la protection des renseignements personnels n'a été aussi essentielle.

Dans ce contexte, la période visée par le rapport a été marquée par des défis croissants au sujet de la protection de la vie privée.

Plus précisément, l'exercice a été marqué par la poursuite d'un débat de longue date au Canada sur l'accès légal aux renseignements personnels des abonnés, ainsi qu'une série de révélations concernant des activités de surveillance de la part de l'État qui avaient des répercussions tant à l'échelle mondiale qu'à l'intérieur de nos frontières.

Les statistiques sont un autre indicateur montrant que le nombre de plaintes a été en augmentation constante. Il en a été de même pour les plaintes déposées par un grand nombre de personnes au sujet d'un seul incident. Par exemple, le Commissariat fait enquête actuellement sur 339 plaintes concernant un envoi massif de Santé Canada qui aurait exposé les noms et les adresses postales d'environ 40 000 participants du Programme d'accès à la marihuana à des fins médicales.

Au cours de 2013-2014, où l'attention accordée aux atteintes à la protection des données dans le secteur public a peut-être été sans précédent, ce sont 228 atteintes distinctes de ce type qui ont été signalées volontairement dans l'ensemble du gouvernement fédéral, soit plus du double comparativement à l'exercice précédent. C'est la troisième année de suite qu'un record de signalements de cette nature est enregistré. La divulgation accidentelle a été donnée comme motif par les organismes déclarants pour expliquer plus des deux tiers des atteintes.

Importantes leçons tirées

L'attention portée aux atteintes à la protection des données au sein du secteur public a été générée en grande partie par la perte d'un disque dur d'Emploi et Développement social Canada (EDSC, alors connu sous le nom de Ressources humaines et Développement des compétences Canada (RHDCC)) qui contenait des renseignements sur plus de 500 000 bénéficiaires de prêts étudiants. Un rapport spécial sur l'incident soumis au Parlement en mars 2014 a fait ressortir qu'il ne s'agit pas seulement,

pour les organisations, d'élaborer des politiques officielles sur la protection des renseignements personnels et la sécurité, mais également de les appliquer et d'assurer une surveillance régulière.

Le Commissariat à la protection de la vie privée du Canada a produit des fiches conseils à l'intention des fonctionnaires sur la façon d'éviter les atteintes à la protection des données lorsqu'ils utilisent des disques durs externes ou d'autres dispositifs portatifs de stockage de données (voir section 5). De plus, le Commissariat vérifie actuellement dans quelle mesure les renseignements personnels stockés sur ces dispositifs portatifs sont protégés dans 17 organismes et ministères.

Comme nous l'avons déjà fait remarquer au cours des années précédentes, étant donné que le signalement au Commissariat des atteintes à la protection des données se faisait sur une base volontaire, le Commissariat n'a jamais pu affirmer de façon catégorique que le nombre d'incidents avait réellement augmenté d'une année à l'autre. L'augmentation pouvait s'expliquer par une plus grande diligence dans le signalement. Désormais, cependant, avec la révision de la *Directive sur les pratiques relatives à la protection de la vie privée* du Secrétariat du Conseil du Trésor (SCT), l'incertitude devrait être moindre.

La Directive rend obligatoire le signalement au SCT et au Commissariat de toute atteinte « substantielle » à la vie privée. Le Commissariat a collaboré avec le SCT à la définition de ce qui constitue une « atteinte substantielle » et à la création d'un formulaire en ligne hébergé sur le site Web du Commissariat qui doit permettre aux institutions fédérales de signaler ces incidents.

Ce travail faisait suite à plusieurs incidents ayant mis en lumière la nécessité d'exercer une vigilance accrue à l'égard de la protection des renseignements personnels détenus par les organisations. Par exemple, le rapport de cette année donne un aperçu de l'enquête menée par le Commissariat sur EDSC et Justice Canada au sujet de la perte d'une clé USB. La clé, qui contenait les renseignements personnels de 5 045 particuliers ayant demandé un nouvel examen de leur admissibilité à des prestations d'invalidité du Régime de pensions du Canada, a disparu d'un bureau d'EDSC où elle était utilisée par un avocat de Justice Canada. Après enquête, le Commissariat a formulé des recommandations qui reprenaient celles formulées dans le rapport spécial publié à la suite de la perte du disque dur contenant les renseignements sur les prêts étudiants.

Enquête de sécurité portant atteinte à la vie privée

Les atteintes à la protection des données sont demeurées au centre des préoccupations en 2013-2014, mais une tendance marquée a été relevée dans les évaluations des facteurs relatifs à la vie privée (EFVP) examinées l'an dernier, à savoir que certaines institutions gouvernementales mettent au point des techniques d'enquête de sécurité qui portent davantage atteinte à la vie privée et vont au-delà de ce qu'exige actuellement le gouvernement fédéral en matière de sécurité. Dans plusieurs cas, ces normes renforcées prévoient la collecte de renseignements personnels dans les médias sociaux et d'autres sources ouvertes.

Par exemple, l'Agence du revenu du Canada (ARC) a soumis une EFVP pour sa norme d'enquête de sécurité sur le personnel au niveau de la « cote de fiabilité+ », qui proposait un certain nombre de nouvelles mesures de vérification plus intrusives, combinant notamment la collecte de renseignements dans les médias sociaux ouverts, la vérification des renseignements contenus dans les dossiers d'application de la loi et les questionnaires de fiabilité. Après avoir consulté le Commissariat, l'ARC a considérablement modifié son programme (pour plus de renseignements à ce sujet, voir la section 5).

Par ailleurs, l'Agence de services frontaliers du Canada (ASFC) a mis en œuvre sa Norme d'intégrité élevée pour les enquêtes de sécurité sur le personnel (sujet présenté dans le rapport annuel de l'an dernier), qui comprend notamment une « entrevue d'intégrité » au cours de laquelle une grande quantité de renseignements personnels est recueillie.

Examen de la GRC

Pendant de nombreuses années, le débat sur l'accès légal a suscité au Canada les discussions les plus animées et importantes concernant la protection de la vie privée. Pour faire progresser ce dossier, le Commissariat a entrepris un examen afin de déterminer si la GRC disposait des contrôles adéquats pour garantir que ses activités liées à la collecte sans mandat de renseignements sur les abonnés auprès d'entreprises étaient conformes à la *Loi sur la protection des renseignements personnels*.

En fin de compte, nous avons été déçus de constater que les lacunes dans la façon dont la GRC consignait ces renseignements nous empêchaient d'évaluer si de tels contrôles étaient en place. Il a été impossible de déterminer à quelle fréquence la GRC recueillait sans mandat des renseignements sur les abonnés ou d'évaluer si ces mesures étaient justifiées. L'examen est présenté à la section 4 du présent rapport.

Surveillance de l'État

Tous les problèmes que nous venons de mentionner sont éclipsés par un enjeu permanent bien plus médiatisé au Canada et dans les autres pays démocratiques, à savoir la préservation, à l'ère numérique, du droit à la vie privée des personnes sans négliger la protection efficace de la sécurité nationale. Les craintes du public sont plus fortes depuis les révélations sur les activités de surveillance de l'État, en particulier parmi les partenaires du « Groupe des cinq », une alliance du milieu du renseignement qui regroupe le Canada, l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les ÉtatsUnis.

Les retombées de ces révélations sont examinées plus en détail dans notre article de fond à la section 3. Nous étudions en particulier leur impact sur les attentes du public, qui souhaite une plus grande transparence de la part des organismes de sécurité quant à leur fonctionnement et à leur utilisation des renseignements personnels, dans la mesure du possible compte tenu du caractère sensible de leurs activités.

Dans son rapport spécial au Parlement de janvier 2014 intitulé *Mesures de vérification et de contrôle : Renforcer la protection de la vie privée et la supervision des activités du secteur canadien du renseignement à l'ère de la cybersurveillance,* le Commissariat s'est penché sur bon nombre de ces questions. Dans la présentation des dix

recommandations détaillées, on pouvait lire ce qui suit :

> *Le but de la revitalisation sur ce front devrait être de protéger la vie privée dans un climat de menaces complexes; de surveiller la collecte pour s'assurer qu'elle est raisonnable, proportionnée et aussi peu envahissante que possible; de veiller à la mise en place de contrôles appropriés concernant la conservation et l'accès (par les intervenants des secteurs public et privé); de veiller à l'exactitude des analyses; et de limiter la portée des demandes et de la communication de renseignements au moyen de mesures de sécurité adéquates, d'ententes et de mises en garde.*

Regard sur l'avenir

En plus des questions relatives à la protection de la vie privée et à la sécurité nationale, le Commissariat suivra de près l'évolution de plusieurs autres facettes de la protection de la vie privée au gouvernement fédéral. Nous nous préoccupons des répercussions négatives possibles sur la vie privée du projet de loi C-13, Loi sur la protection des Canadiens contre la cybercriminalité, qui ont été décrites en détail lors de ma comparution devant le Comité permanent de la justice et des droits de la personne de la Chambre des communes en juin 2014 (voir section 5).

Quelques jours plus tard, la Cour suprême du Canada a déterminé qu'il existe bien une attente raisonnable en matière de respect de la vie privée à l'égard des renseignements des abonnés aux services Internet (*R. c. Spencer*). La Cour suprême a convenu que ces renseignements pourraient, très souvent, constituer la clé permettant l'accès à des renseignements confidentiels sur les activités en ligne d'un utilisateur et, donc, qu'ils méritent d'être protégés par la Constitution.

Le Commissariat suivra de près l'évolution du projet de loi C-13 pour voir quel impact ses recommandations et l'arrêt de la Cour suprême auront sur l'approche adoptée par le gouvernement. Nous ferons également un suivi des atteintes à la protection des données dans les ministères et les organismes gouvernementaux pour évaluer l'effet des nouvelles règles en matière de signalement obligatoire.

Accent maintenu sur la frontière

L'année prochaine, la frontière entre le Canada et les États-Unis demeurera l'un de nos principaux centres d'intérêt. Dans la déclaration de 2011 intitulée Par-delà la frontière et le Plan d'action 2012 sur la sécurité du périmètre, le gouvernement du Canada s'est engagé à l'égard d'une vision renforcée de la sécurité continentale qui faciliterait la circulation des personnes et des biens à la frontière.

Au sens du Plan d'action, la poursuite du déploiement de l'initiative sur les entrées et les sorties signifie que le dossier d'entrée d'un voyageur qui quitte le Canada pour entrer aux États-Unis par un poste frontalier terrestre devient automatiquement son dossier de sortie de notre pays. Avant les premières étapes du programme dans le cadre duquel on a déjà commencé à recueillir les données sur les sorties des ressortissants étrangers et des résidents temporaires, le Canada n'avait jamais recueilli ces renseignements.

L'ASFC a justifié les premières phases du programme en affirmant qu'elles étaient nécessaires à l'exécution des lois en matière

d'immigration. Dans les phases qui suivront, le programme devrait recueillir des renseignements sur tous les citoyens du Canada et des États-Unis qui traversent la frontière, peu importe le mode de transport. À la dernière étape du programme, les données sur les sorties de tous les voyageurs qui quittent le Canada par avion pour n'importe quelle destination seront saisies. En sa qualité d'autorité responsable du programme, l'ASFC a maintenant l'intention d'élargir nettement l'échange des données de sortie au sein du gouvernement, de sorte que ces données puissent être utilisées pour assurer l'intégrité des programmes de prestations sociales, aux fins de l'impôt, aux fins générales d'exécution de la loi et aux fins du renseignement.

À mesure que les détails de ces programmes se précisent, le Commissariat s'attend à ce que l'ASFC et tout ministère participant soumettent des EFVP sur ces nouvelles utilisations proposées des renseignements personnels, qui démontrent que toute répercussion négative éventuelle sur la vie privée est dûment prise en compte (voir section 5). Il exhortera également le gouvernement à faire preuve d'une transparence totale à l'égard des usages prévus, y compris la manière dont les données contenues dans ces dossiers pourraient être combinées à d'autres données recueillies.

Pour conclure

Comme je l'ai mentionné, je n'étais pas commissaire au cours de la période 20132014. Je tiens donc à saluer les efforts et les réalisations de Jennifer Stoddart qui m'a précédé à cette fonction au cours d'une décennie marquée par des défis croissants et riche en accomplissements. J'en profite également pour rendre hommage à Chantal Bernier qui, après avoir été commissaire adjointe à la protection de la vie privée de 2008 à 2013, a été nommée commissaire par intérim après le départ de M^{me} Stoddart.

Sous la direction de M^{me} Stoddart, le Commissariat avait entrepris la définition des domaines stratégiques prioritaires afin d'orienter ses efforts proactifs, ce qui a été très utile à l'organisation pendant plusieurs années.

Avant que je me joigne au Commissariat, un plan avait été établi de façon à revoir la situation et à cerner les priorités stratégiques des quelques années à venir.

Nous amorçons actuellement un travail d'établissement des priorités pour nous aider à cibler les questions de protection de la vie privée qui comptent le plus pour les Canadiennes et les Canadiens. Dans le cadre de cette initiative, nous rencontrerons divers intervenants et groupes afin de connaître leur avis.

Alors que je poursuis la première année de mon mandat de commissaire, j'attends avec intérêt de répondre aux priorités des Canadiens en matière de protection de la vie privée dans un contexte de plus en plus exigeant. Par bonheur, je serai appuyé dans ce travail par une équipe talentueuse et compétente, qui se voue à la protection du droit à la vie privée des Canadiennes et des Canadiens.

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

Daniel Therrien

La protection de la vie privée en chiffres – 2013-2014

Demandes de renseignements reçues au titre de la *Loi sur la protection des renseignements personnels*	**2 147**
Plaintes acceptées (accès, délais, protection des renseignements personnels)	**1 777**
Plaintes fermées à l'issue d'un processus de règlement rapide (accès, délais, protection des renseignements personnels)	**345**
Plaintes fermées à l'issue d'une procédure d'enquête régulière (accès, délais, protection des renseignements personnels)	**1 740**
Examens des EFVP présentant un risque élevé	**65**
Examens des EFVP présentant un risque faible	**36**
Vérifications dans le secteur public déposées	**2**
Communication par des organisations fédérales de renseignements pour des raisons d'intérêt public en vertu de l'alinéa 8(2)(*m*)	**296**
Lois ou 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	**35**

Comparutions devant des comités parlementaires au sujet de questions touchant le secteur public	**5**
Mémoires officiels présentés	**4**
Autres contacts avec des parlementaires ou leur personnel (par exemple correspondance avec des députés ou des sénateurs)	**28**
Discours et exposés présentés	**107**
Visites sur le site Web principal du Commissariat	**2 080 099**
Visites sur les blogues et sur la chaîne YouTube du Commissariat **Visites sur les blogues –** **Visites sur la chaîne YouTube –**	 **623 163** **21 842**
Tweets envoyés	**235**
Abonnés sur Twitter au 31 mars 2014	**7 636**
Publications distribuées	**5 709**
Communiqués de presse et annonces publiés	**25**

3

Article de fond

Des révélations sur la surveillance à un arrêt historique de la Cour suprême du Canada : douze mois où la vie privée a été à l'avant-scène

Nous nous proposons d'examiner ici ce qui a été incontestablement le fait le plus marquant du domaine de la protection de la vie privée l'an dernier au Canada, et de nous intéresser à la genèse de l'une des principales manchettes de l'année à l'échelle internationale — tous secteurs confondus.

De juin 2013 à juin 2014, des termes tels que « métadonnées » et « Groupe des cinq », qui étaient jusqu'ici presque exclusivement utilisés sur des blogues lus par des technologues spécialistes des questions de vie privée et des experts stratégiques, se sont rapidement retrouvés à la une des journaux et au centre de l'actualité. Et si les révélations sur la surveillance de l'État ont donné un aperçu sans précédent des activités des services de renseignement, elles ont aussi soulevé des questions importantes appelant une plus grande transparence, questions qui demeurent d'actualité.

La période de douze mois comprise entre juin 2013 et juin 2014 a débuté en nous laissant entendre que notre vie privée pourrait être assaillie de toutes parts, de façon irrémédiable, et elle s'est terminée par un arrêt de la Cour suprême du Canada reconnaissant qu'une attente raisonnable en matière de respect de la vie privée existe à l'égard des renseignements des abonnés aux services Internet tels que les adresses IP. Entre ces deux moments, il y a eu une multitude de rebondissements.

Dans toute cette période, les Canadiennes et les Canadiens ont montré sans équivoque qu'ils voient la protection de la vie privée comme étant essentielle. En même temps, il est impossible d'ignorer qu'ils considèrent aussi la protection de leur sécurité et de leur sûreté par le gouvernement comme une priorité.

Au final, il ne s'agit pas de choisir entre l'un ou l'autre de ces deux objectifs — il est possible de respecter les deux. Et les Canadiens veulent

une plus grande transparence afin de pouvoir s'assurer du respect suffisant de ces objectifs.

Regarder en arrière et évaluer l'impact

En juin 2013, des renseignements classifiés de nature très technique ont commencé à être tirés de documents fournis à des médias par Edward Snowden, ancien consultant de la National Security Agency (NSA), l'organisme du gouvernement américain responsable du renseignement d'origine électromagnétique.

Dans les mois qui ont suivi, d'autres communiqués ont révélé des opérations secrètes menées par la NSA pour surveiller les communications privées de dirigeants de pays du monde entier. L'existence d'une capacité considérable de saisie, de stockage et d'analyse des métadonnées sur les communications privées et les transactions sur Internet a également été révélée — tout cela en vue de savoir précisément où et quand les conversations ou les échanges ont eu lieu entre des personnes, peu importe où elles se trouvent dans le monde.

Les révélations ont également mis au jour certaines mesures prises par les quatre autres pays membres du « Groupe des cinq » — soit l'Australie, le Canada, la Nouvelle-Zélande et le Royaume-Uni — dont les services du renseignement collaborent et échangent des informations avec leurs équivalents américains.

Le contenu des documents faisait état de certaines activités de l'organisme canadien responsable du renseignement d'origine électromagnétique, le Centre de la sécurité des télécommunications du Canada (CSTC), activités qui allaient de la surveillance des communications de dirigeants de pays du monde entier au Sommet du G20 à Toronto à la surveillance de personnes en 2009 dans un aéroport canadien (dont le nom n'est pas révélé).

Les révélations ont été très médiatisées et ont fait l'objet de débats intenses et constants au Parlement. Au cours de la 2e session de la 41e législature (du 16 octobre 2013 au 19 juin 2014), les parlementaires ont posé plus de 50 questions au sujet du CSTC à la Chambre des communes et au Sénat.

Mettre l'accent sur la supervision des activités du secteur du renseignement

Alors que la surveillance était au centre d'un intense débat parlementaire et à la une des médias, les rouages de cette surveillance ont été examinés de près. Une question, cependant, dominait toutes les autres, soit l'éternelle question de savoir qui surveille ceux qui surveillent. Et une autre : « Comment les parlementaires et les Canadiens qu'ils représentent étaient-ils informés de la manière dont cette supervision s'effectue et dont les résultats sont obtenus? »

La question de la supervision des activités du secteur du renseignement a mis en lumière le rôle du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST), l'organisme chargé de surveiller les opérations du CSTC, et le rôle du Comité de surveillance des activités de renseignement de sécurité (CSARS), l'organisme chargé de surveiller les opérations du Service canadien du renseignement de sécurité (SCRS).

Au début de décembre, le Comité sénatorial de la sécurité nationale et de la défense a tenu des audiences sur la supervision des activités de renseignement. Il a d'abord rencontré le Commissariat à la protection de la vie privée du Canada, le BCCST et le CSARS, puis les dirigeants du CSTC et du SCRS, ainsi que le conseiller à la sécurité nationale auprès du Premier ministre.

Le 9 décembre 2013, Chantal Bernier, commissaire à la protection de la vie privée par intérim, a témoigné au sujet des incidences sur la vie privée de l'échange d'informations entre les services de renseignement du Canada. Elle a rappelé au Comité sénatorial que les dirigeants du BCCST et du CSARS se sont exprimés publiquement sur leur incapacité, aux termes de la loi, à examiner de façon conjointe l'échange d'informations à grande échelle entre les membres du milieu du renseignement.

Cette lacune s'est manifestée en partie parce que, contrairement aux organismes qu'ils surveillent, les deux organismes de surveillance sont encadrés par des limites strictes en matière de règlement et de sécurité pour ce qui est de leurs modes de collaboration.

En janvier 2014, le Commissariat a déposé un rapport au Parlement intitulé *Mesures de vérification et de contrôle : Renforcer la protection de la vie privée et la supervision des activités du secteur canadien du renseignement à l'ère de la cybersurveillance*. Son objectif général était d'informer et de favoriser un débat public plus large sur les questions touchant la surveillance des activités du secteur du renseignement et la transparence. Dans le rapport, le Commissariat a recommandé, entre autres, que le gouvernement aborde les préoccupations déjà exprimées par les organismes de surveillance quant à leur capacité à procéder à des examens conjoints.

Le Comité sénatorial devrait clore ses audiences et publier un rapport plus tard en 2014.

Mesures de vérification et de contrôle : Renforcer la protection de la vie privée et la supervision des activités du secteur canadien du renseignement à l'ère de la cybersurveillance : https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_f.asp

Révéler le parcours de l'information entre le secteur privé et le secteur public

Si les révélations sur la surveillance de l'État ont donné aux citoyens un aperçu sans précédent de cet univers très opaque qu'est le renseignement, elles ont également mis en lumière un élément qui a touché de plus près la plupart des Canadiens. Le 5 juin 2013, parmi les révélations, il y a d'abord eu des renseignements sur Verizon, fournisseur de services de télécommunications, qui a été tenu légalement par la NSA de remettre chaque jour un double des registres d'appels de tous ses abonnés, ce qui a ouvert le débat public sur les métadonnées.

La même semaine, des informations sont sorties sur le programme PRISM de la NSA, soit des documents qui décrivaient en détail la capacité de l'agence à exploiter les données des principaux fournisseurs de services Internet, y compris bon nombre de fournisseurs chez lesquels des Canadiens avaient des comptes de courrier électronique et de réseautage social.

Quelques jours plus tard, au Canada, les médias ont parlé du programme de métadonnées propre au CSTC. Un article du *Globe and Mail a* rapporté en effet que dans le cadre de ce programme, le CSTC

intercepte « accidentellement » les communications des Canadiennes et des Canadiens, mais que lorsque cela se produit, il prend soin de purger ou d'« anonymiser » les données après les avoir obtenues.

Les informations relayées par les médias ont enrichi la discussion sur la protection de la vie privée en ligne. Dans les mois qui ont suivi, le Commissariat a commandé une analyse pour étudier le statut juridique des métadonnées.

https://priv.gc.ca/metadonnees

Si les organismes de sécurité des deux côtés du 49e parallèle soutiennent que la collecte et l'analyse de masse de métadonnées doivent être distinguées du balayage du courriel d'un particulier ou de l'écoute d'une conversation, cela permet à tout le moins d'enregistrer des données telles que le moment où une communication a eu lieu, à partir de quel endroit et avec qui. La collecte de données de cette nature sur une longue période peut ébaucher le profil des activités et de la vie sociale des personnes concernées. C'est pourquoi dans notre analyse nous concluons que dans de nombreux cas, les tribunaux ont reconnu que les métadonnées peuvent révéler beaucoup de choses concernant un individu, et qu'elles méritent d'être protégées, reconnaissant par le fait même que l'importance du contexte.

Quelques notions de base sur les métadonnées

En termes simples, les métadonnées sont des données qui donnent de l'information sur d'autres données. Toutefois, comme un document technique et juridique du Commissariat l'explique clairement, la question est plus complexe qu'il n'y paraît.

Chaque communication électronique, par téléphone ou par courriel, génère des métadonnées. Par exemple, le seul fait d'envoyer un courriel peut produire une douzaine de métadonnées différentes telles que les noms et les adresses courriel de l'expéditeur et du destinataire, l'objet du message, la priorité et le statut.

L'adresse IP de l'expéditeur est également exposée et si on l'associe à d'autres données de base sur les abonnés des services de télécommunications, il est possible de déterminer quels sont les intérêts de la personne, ses penchants idéologiques, les personnes qu'elle fréquente et ses destinations de voyage. En fait, comme le montre clairement le document du Commissariat, les métadonnées peuvent parfois fournir plus d'informations que le contenu réel d'une communication.

Le fait que les métadonnées peuvent contribuer fortement à la destruction de l'anonymat est encore plus préoccupant. Par exemple, à l'aide d'un moteur de recherche de métadonnées, un journaliste de Vancouver a pu établir un profil précis d'une jeune fille de 16 ans uniquement à partir d'un tweet sélectionné de façon aléatoire et géolocalisé.

Le document du Commissariat décrit l'évolution rapide de la définition des métadonnées par les tribunaux, qui ont finalement émis l'opinion juridique selon laquelle, dans de nombreux cas, les métadonnées peuvent permettre de découvrir, en procédant par déductions, comment une personne se comporte ou ce qu'elle fait. Le caractère sensible des métadonnées sur le plan du respect de la vie privée et leur omniprésence font en sorte qu'elles doivent être manipulées avec prudence par le secteur privé et le secteur public.

Quantifier les divulgations sans mandat

En avril 2014, quelques mois après les reportages sur la collecte de métadonnées par la NSA et le CSTC, les préoccupations au sujet de la protection de la vie privée ont été encore attisées par la divulgation de la fréquence avec laquelle les fournisseurs canadiens de services de télécommunications ont transmis des renseignements sur les abonnés aux autorités, sur simple demande et en l'absence d'un mandat. Les données regroupées des compagnies de télécommunications qui ont été fournies au Commissariat par un cabinet d'avocats représentant neuf sociétés de télécommunications indiquaient que 1,2 million de demandes de ce type ont été faites par des enquêteurs en 2011, soit en moyenne plus de 3 200 par jour.

Par ailleurs, le Commissariat a lancé un examen des demandes d'accès sans mandat de la GRC l'an dernier. L'examen visait à déterminer si la GRC avait mis en place des mesures de contrôle adéquates, y compris des politiques, des procédures et des processus, pour garantir que sa collecte sans mandat de données sur les abonnés était conforme aux articles 4 et 5 de la *Loi sur la protection des renseignements personnels*.

En outre, nous espérions parvenir à une plus grande transparence en obtenant la réponse aux questions suivantes :

- À quelle fréquence la GRC recueille-t-elle sans mandat des données sur les abonnés?
- La GRC avait-elle une justification valable pour demander un accès sans mandat aux données sur les abonnés?

Puisque que les systèmes de gestion de l'information de la GRC n'ont pas été conçus pour identifier les dossiers contenant des demandes de divulgation sans mandat d'informations sur les abonnés, nous n'avons pas été en mesure d'établir un échantillon représentatif de dossiers pour examen. Par conséquent, nous n'avons pas pu évaluer le caractère suffisant des mesures de contrôle qui pourraient exister ou encore déterminer si la collecte d'informations auprès des fournisseurs de services de télécommunication au moyen de demandes sans mandat respectait ou non les exigences de la *Loi sur la protection des renseignements personnels* en matière de collecte.

En outre, nous n'avons pas pu déterminer :

- la fréquence à laquelle la GRC recueille sans mandat des données sur les abonnés;
- si la GRC avait une justification valable au sens de la *Loi sur la protection des renseignements personnels* pour demander des données sur les abonnés en l'absence d'un mandat.

Le Commissariat a donc recommandé, pour favoriser une plus grande transparence en ce qui concernant les demandes sans mandat de renseignements sur les abonnés faites par la GRC auprès des fournisseurs de services de télécommunication, que la GRC mette en place un mécanisme lui permettant de surveiller la collecte de renseignements et d'en rendre compte. Bien que l'examen portait principalement sur la GRC, toutes les institutions fédérales devraient appliquer la recommandation qui en découle.

Le texte complet de l'examen se trouve à la section 4 du présent rapport.

Dans les semaines qui ont suivi les rapports sur les 1,2 million de demandes relatives aux télécommunications, le Comité permanent de la justice et des droits de la personne de la Chambre des communes a amorcé les audiences sur le projet C-13, dernière tentative fédérale en matière de loi sur « l'accès légal ».

Lorsque le projet C-13 a été présenté pour la première fois en novembre 2013, le Commissariat avait noté qu'il ne contenait pas la disposition vivement critiquée dans les précédents projets de loi, à savoir une clause visant à contraindre les compagnies de télécommunications à fournir aux autorités, sur demande et sans mandat, des renseignements sur les abonnés. Toutefois, le projet C-13 suscitait d'autres inquiétudes, y compris en ce qui a trait au seuil d'autorisation relativement faible prévu pour l'obtention d'un mandat dans certains cas et à une nouvelle clause d'immunité qui, comme le commissaire Daniel Therrien l'a expliqué lors de sa comparution du 10 juin devant le Comité, « pourrait entraîner une augmentation du nombre de divulgations volontaires et de demandes informelles ».

La transparence favorise la confiance

Lorsqu'il a témoigné concernant le projet de loi C-13, le commissaire Therrien a également affirmé que « les Canadiens s'attendent à ce que leur fournisseur de services préserve le caractère confidentiel des renseignements les concernant et à ce que ces renseignements personnels ne soient pas communiqués à des autorités gouvernementales sans consentement explicite, autorité légitime claire ou mandat. »

La nature profonde de la vie privée réside dans la capacité des personnes à contrôler leurs renseignements personnels. Cette capacité repose essentiellement sur la transparence, un thème qui, l'an dernier, a largement dominé les débats sur les enjeux relatifs à la protection de la vie privée dans le secteur public.

De part et d'autre, les défenseurs des points de vue opposés dans le débat déclenché par les révélations sur la surveillance ont convenu que, dans l'ensemble, les données divulguées n'étaient que de simples aperçus des activités et qu'on ne disposait pas de la vue d'ensemble.

Faire preuve de plus d'ouverture concernant leurs activités, dans la mesure du possible en tenant compte du caractère délicat de chacune d'elle, permettrait aux agences nationales de la sécurité et du renseignement de dissiper les craintes des Canadiens et de gagner leur confiance. Ces efforts contribueraient à l'atteinte d'un important objectif, soit renforcer la confiance de la population canadienne à l'égard des activités des agences nationales responsable de la sécurité.

Cela permettrait également à ces organisations de répondre aux attentes des Canadiens créées par l'ère de l'information que nous vivons.

Toutefois, même si l'on admet qu'un certain degré de confidentialité sera toujours un aspect nécessaire de leurs activités, les services de renseignement ont été plus lents à élever leurs niveaux de transparence.

Dans une lettre adressée à John Foster, chef du CSTC, l'ancienne commissaire à la protection de la vie privée, Jennifer Stoddart, a rappelé la nécessité d'une plus grande transparence, soulignant que « l'ouverture et la responsabilité des gouvernements sont un but louable, peu importe la situation, et elles sont essentielles pour gagner et conserver la confiance des citoyens ». Dans sa réponse, le CSTC s'est engagé à mettre ses fichiers de renseignements personnels (les descriptions de renseignements personnels détenus par des organisations fédérales qui sont consultables à des fins administratives) en ligne (ce qu'il a fait en 2013) et il a commencé à bonifier le contenu sur son site Web, fournissant aux Canadiens davantage d'informations sur la manière dont le CSTC travaille.

En janvier 2014, le rapport spécial *Mesures de vérification et de contrôle* a appelé à la mise en place d'autres moyens pour améliorer la transparence des activités de renseignement menées par des institutions fédérales canadiennes.

Un appel international à une transparence accrue

À la 35e Conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu en septembre 2013 à Varsovie, en Pologne, le Commissariat a adopté et émis, avec d'autres organismes de protection des données, une résolution appelant les organismes fédéraux à une plus grande ouverture. https://www.priv.gc.ca/resource/int/conf_13_f.asp

La protection de la vie privée plus que jamais à l'avant-scène et un arrêt historique

Rétrospectivement, il est difficile de se souvenir d'une seule année où les questions relatives à la protection de la vie privée ont été aussi omniprésentes dans les médias et au Parlement.

En plus des révélations sur la surveillance en tant que telles, le Commissariat a noté un regain d'intérêt général, de la part des médias, pour la protection de la vie privée. Les appels des médias au Commissariat ont augmenté de 40 % entre le 1er avril 2013 et le 31 mars 2014, comparativement à la même période l'année précédente. Et cette augmentation a précédé l'information sur les 1,2 million de demandes d'accès faites aux compagnies canadiennes de télécommunications, qui a suscité un intérêt sans précédent chez les journalistes.

Un peu plus d'un an après le début des révélations sur la surveillance, cette période intense de douze mois a été marquée par un arrêt historique de la Cour suprême confirmant le droit à la vie privée dans *R c. Spencer*.

La Cour suprême a déterminé qu'il existe bien une attente raisonnable en matière de respect de la vie privée à l'égard des renseignements des abonnés des compagnies de télécommunications lorsque ces renseignements permettraient d'accéder à des renseignements confidentiels sur les activités en ligne d'un utilisateur. Par conséquent, contrairement aux

Conséquences globales de l'arrêt Spencer

Quelques principes essentiels de politique et certaines leçons fondamentales sur la protection de la vie privée ont été renforcés par l'arrêt de la Cour suprême, notamment :

a) l'accès légal et les perquisitions des autorités ne peuvent être régis uniquement en fonction de la nature des données consultées de façon isolée; ce que les renseignements recueillis peuvent révéler à leur tour doit également être considéré comme un élément crucial [paragr. 26, 30-33];

b) le caractère intrusif d'une perquisition doit être déterminé en fonction des conséquences possibles sur la personne, et non du caractère illégal du matériel recherché ou de la nature de l'activité criminelle contrecarrée [paragr. 18, 36];

c) les conceptions contemporaines du caractère privé des renseignements personnels tels qu'ils sont protégés par la *Charte* doivent englober les aspects de la confidentialité, du contrôle et de l'anonymat [paragr. 38];

d) pour une grande part, les citoyens échangent entre eux, dans le monde réel et virtuel, des renseignements, sur la foi que ces idées et ces opinions ne seront pas consignées ni rattachées à eux [paragr. 42-43, 45].

Depuis l'arrêt, un grand nombre de compagnies canadiennes de télécommunications ont adopté de nouvelles politiques dans lesquelles elles s'engagent à ne fournir aux autorités des renseignements sur leurs abonnés que lorsque les demandes d'accès aux renseignements auront été autorisées par les tribunaux.

De plus, à la suite des révélations sur la surveillance, beaucoup de fournisseurs de services Internet ont commencé à publier des rapports de transparence annuels dans lesquels ils divulguent le nombre de demandes de renseignements sur les abonnés qui leur sont transmises par les autorités.

renseignements contenus dans un simple bottin téléphonique, un nom et une adresse associés à une adresse IP méritent d'être protégés par la Constitution. Concrètement, cela signifie que sans circonstances contraignantes ou une loi raisonnable prévoyant une autorité légitime, les autorités doivent d'abord obtenir l'autorisation d'un tribunal pour recueillir de tels renseignements.

Le Commissariat a accueilli cet arrêt avec une immense satisfaction puisqu'il confirme le caractère sensible des renseignements des abonnés et reconnaît l'aggravation des risques pour la vie privée depuis le début de l'ère Internet. En outre, il offre aux organismes d'application de la loi et aux fournisseurs de service de télécommunication des éclaircissements qui leur permettent d'ajuster leurs processus et pratiques en conséquence.

Se tourner vers l'avenir

L'année qui vient de s'écouler a été ponctuée par des révélations que certains ont jugées préoccupantes, voire inquiétantes, sous l'angle de la vie privée, mais tout cela a débouché sur des changements positifs qui ont permis au public et aux décideurs d'avoir une idée plus précise de la manière dont les renseignements personnels peuvent être recueillis par les autorités.

Toutefois, il reste des questions importantes sur l'utilisation que font les autorités de ces renseignements, ce qui nécessite une plus grande transparence, de la part non seulement des entreprises du secteur privé, mais également des organismes du secteur public. Sur ce front également, l'année qui vient de se terminer pourrait avoir amené une lueur d'espoir, comme le montre le témoignage du chef du CSTC, John Forster, devant le Comité sénatorial de la sécurité nationale et de la défense, en janvier 2014. Observant que le CSTC est une organisation qui « a évolué dans l'ombre pendant des dizaines d'années », Foster a poursuivi en déclarant :

> « L'un des défis que je dois relever à titre de chef de cette organisation tient au fait que nous devons faire preuve d'une transparence et d'une ouverture bien plus grandes qu'auparavant, et ce, dans les limites qu'impose la réalité que nos activités sont liées à la sécurité nationale. Nous croyons que cela est important, car il s'agit d'une autre façon de renforcer la confiance du public à l'égard de notre travail. »

Robert Décary, ancien commissaire du CSTC, avait exprimé une opinion assez semblable dans son rapport annuel de 2013, où il affirmait au sujet des activités de renseignement : « Plus la transparence sera grande, plus le scepticisme et le cynisme de la population iront s'atténuant ». La même position a été reprise par le commissaire actuel du CSTC, Jean-Pierre Plouffe, qui a indiqué dans son premier rapport annuel que « [l]a transparence est importante pour conserver la confiance du public. […]Mon intention est de poursuivre le travail amorcé par mon prédécesseur afin d'être plus transparent et de donner plus d'information concernant les activités de mon bureau et du CSTC. »

Les derniers mois de l'année ont effectivement apporté des raisons d'espérer que l'intérêt plus vif du public et le débat plus poussé puissent mener à une transparence accrue et à une sécurité renforcée pour les renseignements personnels au cours de l'année qui vient.

Au moment de rédiger le présent rapport, un projet de loi déposé au Parlement, soit une nouvelle mouture du projet de loi C-13 déjà mentionné, pourrait avoir des répercussions importantes sur la protection de la vie privée. Il contient des mesures permettant aux organisations de plus facilement répondre aux demandes des autorités lorsqu'on leur soumet des demandes d'accès aux renseignements des abonnés.

À l'heure actuelle, nous craignons que les mesures proposées n'entraînent des divulgations excessives à l'insu des personnes concernées et du Commissariat.

Afin de nous préparer aux comparutions futures devant le comité qui étudie ce projet de loi, nous étudions la meilleure façon de communiquer aux parlementaires l'importance de l'arrêt Spencer et de la transparence du gouvernement pour renforcer et maintenir la confiance des citoyens.

4 Examen de la Gendarmerie royale du Canada — Accès sans mandat aux renseignements des abonnés

Section 37 of the *Privacy Act*

Introduction

Depuis plus d'une décennie, le gouvernement du Canada étudie diverses propositions qui permettraient à certains organismes gouvernementaux désignés d'obtenir les renseignements personnels détenus par les fournisseurs de services de télécommunications (FST). Depuis 2005, ces propositions d'accès légal ont été exposées dans huit projets de loi distincts déposés par le gouvernement du Canada. Au moment de la rédaction du présent rapport (octobre 2014), le Parlement envisage toujours d'adopter une loi qui moderniserait les techniques d'enquête policière, mais une telle loi serait lourde de conséquences pour la protection de la vie privée en ligne. Au moment de la rédaction du présent rapport, le projet de loi C 13, la Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle (également connue sous le nom de Loi sur la protection des Canadiens contre la cybercriminalité), en était à l'étape du rapport devant la Chambre des communes.

Les représentants des organismes canadiens d'application de la loi demandent depuis un certain temps que de nouveaux pouvoirs de police soient codifiés dans une loi sur l'accès légal. Ils ont signalé que l'utilisation d'Internet et l'évolution des infrastructures de télécommunications au Canada ont créé des obstacles aux enquêtes. Pour remplir les responsabilités prévues à leur mandat, les organismes d'application de la loi cherchent à repérer les activités criminelles et ceux qui les mènent sur Internet, dans le contexte d'une enquête licite. En conséquence, ces organismes peuvent demander l'accès aux renseignements des abonnés pour un vaste éventail d'enquêtes criminelles, notamment l'exploitation des enfants, la drogue et le crime organisé, les enlèvements, la cyberintimidation et les crimes financiers, ainsi que d'autres situations d'urgence en matière de sécurité publique, comme les menaces de suicide et les disparitions. Les exigences légales pour obtenir des renseignements sur les abonnés varient selon la nature des renseignements recherchés.

L'information demandée varie aussi : elle peut se limiter au nom et à l'adresse liés à un numéro de téléphone ou inclure le nom associé à une adresse de protocole Internet (IP).

Importance pour les Canadiens

Le public est très attentif à la surveillance du gouvernement et aux demandes de renseignements sur les abonnés que font les organismes d'application de la loi sans autorisation judiciaire préalable.

Avant l'arrêt *R.* c. *Spencer* de la Cour suprême du Canada, de nombreux FST ont communiqué des renseignements sur les abonnés à des organismes d'application de la loi qui les demandaient sans avoir obtenu au préalable d'autorisation judiciaire. Certaines de ces demandes portaient sur de l'information susceptible de permettre à des organismes gouvernementaux d'avoir accès à des renseignements qui pourraient être associés par la suite à des renseignements personnels et à d'autres renseignements de nature confidentielle, notamment l'utilisation d'Internet.

Cette pratique des organismes d'application de la loi qui consiste à demander des renseignements sur les abonnés sans autorisation judiciaire n'est pas bien comprise par les Canadiennes et les Canadiens. En fait, ils sont mal informés concernant ces demandes, y compris la fréquence à laquelle elles ont été faites, et le type de renseignements recherchés.

C'est dans ce contexte que le Commissariat a décidé de procéder à un examen de la Gendarmerie royale du Canada (GRC), de façon à faire la lumière sur cette pratique qui consiste à obtenir sans mandat des renseignements sur les abonnés auprès des FST.

Au sujet de la GRC

La GRC agit sous l'autorité de la *Loi sur la Gendarmerie royale du Canada.* Un commissaire dirige l'organisation qui relève du ministre de la Sécurité publique Canada. Rappelons que la GRC est le corps policier le plus important du Canada dont le vaste mandat englobe des fonctions internationales et nationales.

La GRC fait appliquer les lois fédérales dans l'ensemble du pays, et les lois provinciales ou territoriales dans toutes les provinces et tous les territoires, sauf en Ontario et au Québec. Elle fournit également des services de soutien aux enquêtes, aux opérations et aux activités de nature technique à plus de 500 organismes canadiens d'application de la loi et de justice pénale.

La GRC exerce ses activités dans environ 150 municipalités et 600 communautés autochtones, et dans trois aéroports internationaux. Elle compte, au Canada et à l'étranger, près de 29 000 employés, qui sont des membres réguliers et civils, et des fonctionnaires.

Dans l'exécution de son mandat, la GRC recueille une variété de données et demande des renseignements à diverses personnes et sources du secteur public et du secteur privé. Notre examen portait plus particulièrement sur un point : le fait que la GRC, dans les enquêtes menées aux fins de l'application de la loi pourrait demander aux FST des renseignements sur les abonnés sans avoir de mandat.

Contexte

Le 24 octobre 2013, la commissaire à la protection de la vie privée a transmis un avis d'examen au commissaire de la GRC en vertu de l'article 37 de la *Loi sur la protection des renseignements personnels.* Dans cet avis, il était indiqué que le Commissariat mènerait des travaux préliminaires qui pourraient déboucher sur une vérification de la collecte par la GRC, sans mandat, de renseignements sur les abonnés auprès des FST.

Objectif

L'examen avait pour objectif de déterminer si la GRC avait mis en place des mesures de contrôle adéquates, y compris des politiques, des procédures et des processus, pour garantir que sa collecte sans mandat de renseignements sur les abonnés était conforme aux articles 4 et 5 de la *Loi sur la protection des renseignements personnels*.

En outre, nous espérions parvenir à une plus grande transparence en obtenant la réponse aux questions suivantes :

- À quelle fréquence la GRC recueille-t-elle sans mandat des données sur les abonnés?
- La GRC avait-elle une justification valable, au sens de la *Loi sur la protection des renseignements personnels*, pour demander un accès sans mandat aux données sur les abonnés?

Compte tenu des déclarations et des engagements du gouvernement fédéral à l'égard de l'ouverture et de la transparence, nous nous attendions à ce que les dossiers de la GRC permettent de rendre compte des questions susmentionnées.

Observations

La *Loi sur la protection des renseignements personnels* limite la collecte de renseignements personnels par des entités fédérales à ce qui est lié à un programme ou à une activité. Au cours de notre examen, nous voulions évaluer si les demandes d'accès sans mandat aux renseignements sur les abonnés présentées par la GRC aux FST respectaient l'exigence susmentionnée.

Dans le cadre de notre examen, nous avons rencontré plus de cinquante personnes : des dirigeants de la GRC, des agents de terrain qui ont demandé d'avoir accès sans mandat aux renseignements sur les abonnés et des spécialistes des technologies de l'information chargés de gérer et d'extraire les renseignements des bases de données d'enquête de la GRC. Nous avons également interrogé des spécialistes du secteur des télécommunications qui ont l'habitude de ce type de demandes. Enfin, nous avons examiné la politique de la GRC sur l'enregistrement des activités d'application de la loi dans ses bases de données d'enquête.

Cette politique stipule que la collecte et l'utilisation des renseignements opérationnels sont assujetties aux dispositions de la *Loi sur la protection des renseignements personnels*. Bien que les politiques de la GRC ne traitent pas précisément de la demande sans mandat de renseignements sur les abonnés auprès des FST, elles s'appliquent à l'ensemble des activités opérationnelles de la GRC, y compris ce type de collecte.

La GRC nous a signalé qu'environ deux millions de nouveaux incidents sont entrés dans son principal système de gestion des dossiers chaque année. Nous avons fait des recherches dans ce système : ce n'est que dans des cas isolés que nous sommes parvenus à relier les demandes sans mandat de renseignements personnels sur les abonnés aux dossiers contenant de telles demandes. Selon nos observations, à moins d'un examen manuel de chaque dossier, la GRC n'est pas en mesure à l'heure actuelle de produire un rapport comportant la liste, partielle ou complète, des dossiers opérationnels dans le cadre desquels il y a eu un accès sans mandat à des renseignements personnels sur les abonnés, ainsi que la fréquence de telles demandes. La GRC a fait valoir que son système de gestion des dossiers n'est pas conçu à cette fin.

La GRC a affirmé que son système de gestion des dossiers d'enquête opérationnels vise à appuyer les enquêtes et à satisfaire aux exigences légales à l'égard de la transmission à Statistique Canada de certaines données sur la criminalité. Les systèmes n'ont pas été conçus pour rendre compte de tous les cas, de façon regroupée, de demandes d'accès sans mandat de renseignements sur les abonnés. La GRC a aussi fait valoir que la compilation de tels renseignements est compliquée par le fait qu'une affaire criminelle complexe peut comprendre de nombreuses demandes d'accès sans mandat à des renseignements sur les clients (noms et adresses associés à un numéro de téléphone). De plus, la méthode utilisée et le type de renseignements demandés varient selon la nature du dossier et les obligations des FST.

Le Centre national de coordination contre l'exploitation des enfants (CNCEE) de la GRC a été le seul endroit où il nous a été possible d'examiner les dossiers de demandes d'accès sans mandat aux renseignements sur les abonnés. Cependant, les demandes du CNCEE ne représentent qu'un sous-ensemble des demandes effectuées par la GRC. Selon notre examen des dossiers du CNCEE, les demandes d'accès sans mandat aux renseignements sur les abonnés se rapportaient à des enquêtes en cours. Nous ne sommes toutefois pas en mesure d'extrapoler des résultats au-delà du secteur du CNCEE.

La GRC a elle-même reconnu la pertinence de la saisie de données statistiques sur les demandes d'accès sans mandat aux renseignements sur les abonnés. Le 12 janvier 2010, le commissaire adjoint aux opérations techniques a diffusé une note de service pour exiger de ses unités de première ligne qu'elles commencent à documenter les cas de demandes d'accès sans mandat à des renseignements sur les abonnés auprès des FST. La note visait à soutenir la nouvelle présentation possible du projet de loi C-47, Loi sur l'assistance au contrôle d'application des lois au 21e siècle.

Selon la GRC, puisque le projet de loi C-47 n'a pas progressé au-delà de la deuxième lecture au Parlement, la collecte de données n'a jamais été tout à fait opérationnalisée. Toutefois, selon la note de service, le projet de loi avait déjà été à l'étape de la deuxième lecture au Parlement et était mort au Feuilleton au moment de la prorogation de décembre 2009. Selon notre compréhension de la note, et le moment de sa diffusion, la directive donnée aux fonctionnaires de recueillir les données statistiques sur les

demandes d'accès aux renseignements sur les abonnés visait à réunir de l'information pour montrer la nécessité de disposer d'une loi générale sur l'accès légal. De telles mesures législatives ont été proposées de nouveau en novembre 2010, avec le projet de loi C-52, Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention, puis en février 2012, avec le projet de loi C-30, Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois.

Le 13 juin 2014, la Cour suprême du Canada a rendu sa décision dans l'affaire *R.* c. *Spencer*, décision qui a eu un effet direct sur les activités d'examen en cours du Commissariat. Dans ce dossier, l'ensemble de la Cour a constaté l'existence d'une attente raisonnable en matière de respect de la vie privée, au sens de l'article 8 de la *Charte*, pour ce qui est des renseignements sur les abonnés susceptibles de permettre d'établir un lien entre une personne et ses activités en ligne. La Cour a conclu que, dans ce dossier, la police a obtenu l'information de façon inconstitutionnelle puisqu'elle ne détenait pas l'autorité légitime requise pour obtenir de tels renseignements à défaut de circonstances contraignantes ou d'une loi qui n'a rien d'abusif. La GRC a indiqué avoir rajusté ses méthodes d'enquête pour qu'elles se conforment à la décision *Spencer*. Étant donné que le principal système de gestion des dossiers de la GRC n'est pas conçu pour repérer les demandes d'accès sans mandat, et compte tenu de l'impact de la décision de la Cour suprême du Canada (*R.* c. *Spencer*) sur la capacité de collecte sans mandat des données sur les abonnés par la GRC, le Commissariat a décidé de ne pas poursuivre l'examen.

Finalement, notre examen des dossiers et les entrevues que nous avons menées avec le personnel de la GRC ne nous ont pas permis de déterminer si la GRC, dans son ensemble, respectait ou non les dispositions de la *Loi sur la protection des renseignements personnels* pour ce qui est de la collecte sans mandat de renseignements sur les abonnés. Qui plus est, la GRC, à moins de procéder à un examen manuel de chacun des dossiers conservés, n'a aucun moyen de prouver qu'elle agit de façon conforme à cet égard.

Recommandation : *Afin de favoriser la transparence accrue relativement aux demandes d'accès sans mandat aux renseignements sur les abonnés qu'elle présente aux fournisseurs de services de télécommunications, la GRC devrait mettre en place un mécanisme de surveillance et de rapport concernant la collecte de tels renseignements.*

Réponse de la GRC

Les principales responsabilités de la GRC sont de préserver la paix, de prévenir le crime et d'enquêter sur les infractions aux lois du Canada. Dans le cadre de son mandat, la GRC s'engage pleinement à respecter les lois canadiennes, y compris la Loi sur la protection des renseignements personnels. Les systèmes de gestion des documents de la GRC ont été conçus pour répondre à des normes d'enquêtes et de preuves, et non dans le but de présenter des données agrégées sur la source de l'information recueillie durant ses

enquêtes. Cela dit, pour assurer l'adhésion et la conformité aux lois canadiennes, la GRC possède une vaste gamme de politiques, pratiques et normes opérationnelles.

Bien qu'elle s'attende à une diminution du nombre de demandes d'accès sans mandat par suite de la décision dans l'affaire *R.* c. *Spencer*, elle continuera à faire de telles demandes dans des situations particulières, notamment des circonstances contraignantes ou d'une loi qui n'a rien d'abusif. La GRC créera un groupe de travail chargé d'explorer des mécanismes efficaces et économiques qui permettraient de mieux suivre les demandes d'accès sans mandat aux renseignements sur les abonnés et de faire rapport sur ces demandes. Elle présentera un rapport sur la question au comité de vérification ministériel d'ici le mois d'avril 2015.

En outre, comme suite à la décision dans l'affaire *R.* c. *Spencer*, le ministère de la Justice et le Service des poursuites pénales du Canada travaillent avec la communauté interministérielle à examiner la décision et ses répercussions. La GRC s'engage à pleinement respecter toutes les nouvelles exigences une fois que les répercussions de la décision auront été déterminées.

Conclusion

Avec notre examen, nous avons cherché à informer le Parlement et les Canadiens et Canadiennes au sujet du recours, par la GRC, à des demandes d'accès sans mandat aux renseignements sur les abonnés auprès des FST.

Étant donné que les systèmes de gestion des dossiers de la GRC ne sont pas conçus pour repérer les dossiers comportant des demandes d'accès sans mandat aux renseignements sur les abonnés, le Commissariat n'a pas été en mesure d'établir un échantillon représentatif de dossiers aux fins d'examen. En conséquence, il lui est impossible d'évaluer si les mesures de contrôle qui pourraient exister, sont suffisantes, ni si l'accès sans mandat aux renseignements détenus par les FST est conforme ou non aux dispositions de la *Loi sur la protection des renseignements personnels*.

En outre, le Commissariat n'a pas pu déterminer :

- la fréquence de la collecte sans mandat de renseignements sur les abonnés par la GRC;
- si la GRC a une justification valable, en vertu de la *Loi sur la protection des renseignements personnels*, pour demander l'accès sans mandat aux renseignements sur les abonnés.

La tenue de dossiers exacts sur les demandes sans mandat de renseignements sur les abonnés est conforme à l'engagement de transparence pris par le gouvernement du Canada. En outre, la tenue de dossiers exacts pourrait fournir la preuve nécessaire pour justifier la nécessité de mettre en œuvre une loi sur l'accès légal.

AU SUJET DE L'EXAMEN

Autorisation
L'article 37 de la *Loi sur la protection des renseignements personnels* habilite le commissaire à la protection de la vie privée à examiner les pratiques de gestion de renseignements personnels des institutions fédérales.

Objectif
L'examen visait à déterminer si la GRC avait ou non mis en place des mesures de contrôle adéquates, y compris des politiques, des procédures et des processus, pour garantir que sa collecte sans mandat des données des abonnées était conforme aux articles 4 et 5 de la *Loi sur la protection des renseignements personnels*.

Critères
Les critères de l'examen découlaient de la *Loi sur la protection des renseignements personnels* et des politiques, directives et normes du Secrétariat du Conseil du Trésor concernant la gestion des renseignements personnels.

Nous espérions pouvoir conclure que la GRC :

- possède des politiques, des pratiques et des procédures permettant de garantir que les demandes d'accès sans mandat qu'elle fait aux FST ne concernent que les renseignements personnels liés au fonctionnement des programmes;

- a documenté de façon systématique ses demandes d'accès sans mandat auprès des FST, conformément à l'engagement d'ouverture et de transparence du gouvernement du Canada.

Portée et approche
Les activités d'examen se sont déroulées à la Direction générale de la GRC à Ottawa, et avec certains représentants de la GRC de différentes régions du pays.

Le Commissariat a examiné les politiques, les pratiques, les procédures et les fichiers électroniques concernant les demandes d'accès sans mandat. L'examen des dossiers, les entrevues avec 52 représentants, les démonstrations des systèmes et d'autres vérifications d'examen ont permis de rassembler les éléments de preuve.

L'exercice ne comprenait pas d'examen des demandes d'accès avec mandat, par le recours à des traités d'entraide juridique, à des numéros de téléphone ou à des sites qui fournissent des services de recherche sur Internet.

L'examen a débuté le 24 octobre 2013 et a été abandonné en juin 2014 à la lumière de la décision de la Cour suprême du Canada dans l'affaire *R.* c. *Spencer*.

Normes
L'examen a été mené dans le respect du mandat législatif, des politiques et des pratiques du Commissariat à la protection de la vie privée du Canada.

Équipe chargée de l'examen
Steven Morgan
Tom Fitzpatrick
Sylvie Gallo Daccash
Ivan Villafan

5 Bilan de l'année

ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Les évaluations des facteurs relatifs à la vie privée (EFVP) servent à déceler les risques potentiels d'atteinte à la vie privée que posent les programmes ou les services fédéraux nouveaux ou remaniés. Elles aident aussi à éliminer ou à réduire ces risques à un niveau acceptable.

Elles permettent d'étudier en détail la façon dont les institutions gouvernementales fédérales protègent les renseignements personnels qui sont recueillis, utilisés, communiqués, conservés et finalement détruits. Les évaluations contribuent à l'édification d'une culture davantage axée sur la protection de la vie privée dans les ministères fédéraux. Elles doivent être préparées bien avant que l'on lance une nouvelle initiative (ou qu'on apporte des changements à une initiative existante) afin d'aborder les risques tôt et de façon proactive. Les organisations qui font des EFVP une priorité sont gagnantes puisque la possibilité d'incidents indésirables, par exemple, une atteinte à la protection des données, est réduite. De plus, elles font preuve d'un engagement actif à l'égard de la transparence et du respect de la vie privée des Canadiens.

Selon la *Directive sur l'évaluation des facteurs relatifs à la vie privée* du Secrétariat du Conseil du Trésor, les institutions fédérales ont la responsabilité de mener des EFVP pour les activités ou les programmes nouveaux, ou modifiés de façon substantielle, qui impliquent l'utilisation de renseignements personnels pour la prise de décisions touchant des particuliers. Les institutions fédérales doivent démontrer que les risques liés à la protection des renseignements personnels ont été cernés et que des mesures efficaces d'atténuation des risques ont été prises. Le Commissariat reçoit des copies des évaluations pour examen et, le cas échéant, transmet aux institutions des conseils et des recommandations susceptibles d'améliorer leurs pratiques de gestion des renseignements personnels. La plupart des institutions acceptent et suivent nos conseils, mais nos recommandations ne sont pas contraignantes.

Collecte de renseignements au passage à la frontière

Les EFVP examinées par le Commissariat l'an dernier révèlent une tendance à une collecte plus importante de renseignements personnels aux postes frontaliers, et à une expansion de l'échange et de l'utilisation de ces renseignements. Cette surveillance accrue est en grande partie attribuable à l'initiative sur les entrées et les sorties, l'une des initiatives élaborées dans le cadre de l'accord Par-delà la frontière conclu entre le Canada et les États-

Unis sur la sécurité du périmètre. La collecte des données de sortie aux frontières terrestres se base sur un échange entre les deux pays, le dossier d'entrée d'une personne dans un pays devenant automatiquement le dossier de sortie de l'autre pays. Auparavant, le gouvernement du Canada ne recueillait généralement pas les renseignements sur les personnes qui quittaient le pays.

Les phases I et II de l'initiative sur les entrées et les sorties ont consisté en un échange de données entre le Canada et les États-Unis sur les ressortissants de pays tiers et de résidents permanents franchissant les frontières terrestres. Quand il a examiné l'EFVP relative à la phase II, le Commissariat a appris que l'Agence des services frontaliers du Canada (ASFC) avait l'intention de conserver pendant 75 ans les renseignements personnels recueillis dans le cadre de l'initiative. Nous avons demandé à l'ASFC de justifier la période de conservation prévue. Pour donner suite à notre recommandation, l'ASFC a réduit à 30 ans la période de conservation des renseignements, avec dépersonnalisation des renseignements après 15 ans. Nous avons toutefois demandé à l'Agence de justifier la période de conservation des renseignements, et demandé aussi à toutes les autres institutions qui recueilleront également ces renseignements de justifier à leur tour la durée de conservation. À cette date, nous attendons encore cette justification.

Si l'initiative va de l'avant, la phase III étendra la surveillance aux citoyens canadiens et américains qui passent par la frontière terrestre, et la phase IV comprendra la collecte des données de sortie de tous les voyageurs qui quittent le Canada par avion. Les transporteurs aériens commerciaux seront tenus par la loi de remettre la liste des passagers des vols sortants à l'ASFC. Nous croyons comprendre qu'une nouvelle loi devra être adoptée par le Parlement et qu'il faudra aussi modifier les règlements pour permettre l'extension envisagée par l'ASFC.

L'ASFC a justifié les premières phases de l'initiative en affirmant qu'elles étaient nécessaires à l'intégrité des frontières et à l'application des lois sur l'immigration, indiquant que les opérations d'application de la loi et de renvoi des personnes dépassant la durée de séjour autorisée sur leur visa seraient mieux ciblées si l'Agence avait davantage de renseignements sur les personnes ayant quitté le pays.

Les plans des phases suivantes de l'initiative sur les entrées et les sorties prévoient non seulement la collecte des données de sortie pour tous les voyageurs, mais également l'utilisation de ces renseignements personnels à des fins plus larges. Cela comprend leur utilisation par des organismes d'application de la loi, par Citoyenneté et Immigration Canada (CIC) pour valider les exigences en matière de résidence, et par Emploi et Développement social Canada pour déterminer l'admissibilité à l'assurance-emploi. Les dossiers de sortie pourraient également être partagés avec d'autres ministères tels que la GRC, le Service canadien du renseignement de sécurité (SCRS) et l'Agence du revenu du Canada (ARC). En 2014-2015, le Commissariat compte recevoir des EFVP portant spécifiquement sur les nouvelles utilisations des renseignements personnels recueillis dans le cadre de l'initiative sur les

entrées et les sorties. Nous avons recommandé de faire la démonstration que chacune de ces utilisations plus étendues est nécessaire et efficace, qu'elles soient effectuées de la manière la moins intrusive possible du point de vue de la vie privée et qu'elles soient conçues de façon à ce que toute atteinte à cet égard soit compensée par un bénéfice sociétal substantiel.

Le Commissariat continue de rencontrer des représentants de l'ASFC et d'autres ministères et espère recevoir des EFVP plus détaillées au début de 2015.

Biométrie à la frontière

Une autre initiative gouvernementale soulève un grand nombre de préoccupations du même ordre sur le plan de la protection de la vie privée : le Projet de biométrie pour les résidents temporaires (PBRT), qui est géré conjointement par CIC, l'ASFC et la GRC. Début 2013, des citoyens de 29 pays et d'un territoire qui ont soumis une demande pour visiter le Canada, y étudier ou y travailler ont été contraints de fournir leurs empreintes digitales et de se faire prendre en photo pour leur demande de visa.

Le PBRT a d'abord été présenté au Commissariat comme un moyen d'examiner l'admissibilité des demandeurs, de confirmer leur identité au cours du processus de demande et de vérifier l'identité des titulaires de visas lorsqu'ils sont entrés au Canada. Sur cette base, le gouvernement a démontré que cette vérification constituait un usage adéquat de la biométrie, qui présentait des risques minimes sur le plan de la protection de la vie privée, à condition que des mesures de sécurité valables soient appliquées.

Cependant, le projet a été étendu afin de permettre à la GRC de conserver pendant 15 ans les empreintes et d'autres renseignements recueillis dans le cadre du processus de demande. Ces renseignements pourraient alors être utilisés pour déterminer leur correspondance avec des entrées du répertoire des empreintes digitales des criminels et des empreintes latentes prélevées sur les scènes de crime.

CIC a indiqué que les demandeurs de visas consentent à cette utilisation sur le formulaire de demande qu'ils remplissent. En poursuivant son travail sur les EFVP concernant ce projet, le Commissariat s'est également demandé si les demandeurs de visas sont pleinement informés de l'usage qui pourrait être fait de leurs empreintes. Nous nous sommes également demandé si la durée de conservation des empreintes de personnes qui n'ont été ni accusées ni reconnues coupables d'une infraction criminelle, et si le caractère systématique de la conservation, sont justifiées. Nous avons recommandé à CIC d'examiner soigneusement ses mécanismes de consentement et ses périodes de conservation.

CIC a répondu que si une institution gouvernementale possède des renseignements personnels qui pourraient permettre d'identifier une personne d'intérêt aux fins de l'application de la loi, elle devrait communiquer cette information. Nous avons avisé CIC que c'est une interprétation large de ce qui constitue une divulgation acceptable et que la *Loi sur la protection des renseignements personnels* fixe certaines limites précises quant aux circonstances dans lesquelles des renseignements personnels recueillis par une institution gouvernementale

peuvent être communiqués à un organisme d'application de la loi. Nous continuons à tenir des consultations sur cette initiative avec les ministères concernés.

Enquête de sécurité de l'Agence du revenu du Canada

D'après les EFVP examinées au cours de l'année, il semble y avoir une tendance, à l'échelle du gouvernement, à recourir de plus en plus à des méthodes d'enquête de sécurité plus intrusives pour les candidats à un emploi au gouvernement. Ces méthodes peuvent comprendre la collecte de renseignements personnels sur les médias sociaux et des « vérifications de l'intégrité » qui peuvent consister à poser des questions indiscrètes aux employés potentiels sur des sujets tels que les jeux de hasard, les finances personnelles, les relations et la consommation de drogue ou d'alcool. Ces mesures de contrôle s'ajoutent aux exigences actuelles du gouvernement fédéral en matière de sécurité.

Le processus d'enquête de sécurité du personnel au niveau « cote de fiabilité+ » de l'Agence du revenu du Canada illustre bien cette tendance. Cette méthode de contrôle approfondi s'applique à près de 300 postes, dont l'ARC indique qu'ils exigent un degré élevé d'intégrité et de pouvoir décisionnel. La méthode proposée dans l'EFVP comprenait le prélèvement d'empreintes, les enquêtes de crédit, les vérifications de dossiers des organismes d'application de la loi (plus poussées que les vérifications du casier judiciaire), la vérification de la conformité fiscale, les vérifications dans les sources ouvertes, y compris dans les médias sociaux, et un questionnaire de fiabilité de caractère intrusif à remplir.

Notre examen de l'EFVP nous a permis de cerner les risques, sur le plan de la protection de la vie privée, posés par l'ajout de nombreuses vérifications à caractère intrusif, en particulier le questionnaire de nature très générale pouvant mener à une collecte excessive de renseignements personnels.

À l'issue de nos consultations, l'ARC a revu ou modifié certains des éléments les plus intrusifs du processus de contrôle de sécurité et a entièrement renoncé au questionnaire.

Tribunal de la sécurité sociale

L'an dernier, le gouvernement a changé et regroupé le système servant à entendre les appels sur les décisions relatives à l'assurance-emploi, au Régime de pensions du Canada et à la Sécurité de la vieillesse, sans soupeser pleinement les conséquences sur les plans de la protection et de la sécurité des renseignements personnels de milliers de Canadiennes et de Canadiens.

Par le passé, un conseil composé de plus de 1 000 juges-arbitres à temps partiel entendait les appels interjetés, au sein de comités tripartites travaillant à partir de bureaux du gouvernement. Dans le nouveau système, 74 membres à temps plein d'un Tribunal de la sécurité sociale se prononcent sur des appels dans le cadre d'un régime de télétravail à domicile.

Le Commissariat a reçu une EFVP d'Emploi et Développement social Canada uniquement après que le nouveau tribunal est entré en service en avril 2013. Bon nombre des politiques et des

procédures censées protéger les renseignements personnels des appelants étaient toujours en cours d'élaboration, y compris les mesures de sécurité entourant le télétravail et l'évaluation de la sécurité des bureaux à domicile des membres du tribunal. Au moment de la rédaction du présent rapport, début septembre 2014, le Commissariat n'avait toujours pas reçu les résultats de ces évaluations, qui sont déterminantes pour la prise en compte de tout risque relatif à la protection des renseignements personnels.

ATTEINTES À LA PROTECTION DES DONNÉES

Pour la troisième période consécutive de rapport, le nombre d'atteintes à la protection des données signalées volontairement au Commissariat par les ministères et les organismes a atteint un niveau record.

Toute perte ou communication non autorisée de renseignements personnels constitue une atteinte à la protection des données. Les personnes concernées n'étaient pas toujours au courant de l'atteinte; dans d'autres cas, les personnes ont été officiellement informées ou elles l'ont appris par les médias.

Pourtant, comme le Commissariat l'avait souligné dans ses précédents rapports annuels, nous ignorons s'il y a eu véritablement davantage d'atteintes à la protection des données au cours de l'année visée par le rapport, ou si les institutions les ont signalées avec plus de diligence. Cette incertitude devrait nettement diminuer à l'avenir grâce aux révisions apportées en mai 2014 à la *Directive sur les pratiques relatives à la protection de la vie privée* du Secrétariat du Conseil du Trésor (SCT), qui exige désormais que les institutions fédérales signalent toutes les atteintes substantielles à la protection des données au Commissariat et au SCT.

Soulignons que le Commissariat a collaboré étroitement avec le SCT pour orienter la définition d'une « atteinte substantielle ». Au moment de rédiger le présent rapport, les institutions indiquaient avoir toujours de la difficulté à s'habituer à la nouvelle directive. Depuis qu'elle est en vigueur, il semble que davantage d'atteintes ont été signalées au Commissariat qu'au SCT, alors que les incidents devraient être signalés aux deux organisations.

Même en 2013-2014, lorsque le signalement volontaire prédominait, 228 atteintes à la protection des données à l'échelle du gouvernement ont été signalées au Commissariat, soit plus du double par rapport aux 109 atteintes signalées durant l'exercice précédent. La divulgation accidentelle (c'est-à-dire attribuable à l'erreur humaine) représentait un peu plus des deux tiers de ces atteintes.

Une atteinte particulièrement importante concernait la perte d'un disque dur externe à Emploi et Développement social Canada en 2012. Le disque dur contenait les renseignements personnels de 583 000 bénéficiaires de prêts étudiants.

Dans son rapport d'enquête spécial déposé au Parlement en mars 2014, le Commissariat a expliqué en détail comment le disque dur a été laissé dans un lieu non sécurisé pendant de

longues périodes, n'était pas protégé par un mot de passe et contenait des renseignements personnels non codés. À la suite de l'enquête, le Commissariat a rédigé des conseils à l'intention des institutions fédérales sur l'utilisation des dispositifs de stockage portatifs.

Aucune organisation n'est à l'abri d'une atteinte possible à la protection des données. Même le Commissariat à la protection de la vie privée en a fait l'expérience, avec la perte d'un disque dur contenant des renseignements sur les employés survenue lorsqu'il a déménagé son administration centrale de l'Ontario au Québec. On s'attend à ce que le commissaire spécial à la protection de la vie privée fasse mention de cet incident dans sa contribution au Rapport annuel 2014-2015 du Commissariat concernant la *Loi sur la protection des renseignements personnels*.

Conseils aux institutions fédérales qui utilisent les dispositifs de stockage portatifs
https://www.priv.gc.ca/media/nr-c/2014/nr-c_140325_f.asp

Une fiche-conseils de quatre pages du Commissariat, sur l'utilisation de dispositifs de stockage portatifs, donne aux employés des ministères et des organismes fédéraux une liste de vérification sur les quatre types de contrôle à appliquer pour éviter les atteintes à la protection des données, à savoir les contrôles physiques, technologiques et administratifs, et les contrôles du personnel.

Les contrôles physiques, par exemple, privilégient la protection des dispositifs non utilisés. Ces contrôles consistent à placer les dispositifs dans des classeurs verrouillés ou dans des zones d'entreposage à accès restreint. Les contrôles technologiques comprendraient le chiffrement ou des mots de passe forts, et une formation des employés sur ces deux éléments.

Pour ce qui est des contrôles administratifs, la fiche-conseils recommande d'assigner des numéros de série aux dispositifs afin qu'on puisse en faire le suivi et de n'utiliser de dispositifs de stockage portatifs pour des renseignements personnels qu'en dernier recours.

Les contrôles de sécurité du personnel englobent la formation régulière obligatoire sur la sécurité et la protection des renseignements personnels, et la surveillance de l'utilisation des dispositifs de stockage personnels par les employés, de façon à assurer le respect des politiques et des procédures.

LE PARLEMENT

À titre d'agent du Parlement, le Commissariat apprécie les possibilités de conseiller les parlementaires au sujet des conséquences, sur le plan de la protection de la vie privée, des lois et des questions qu'ils étudient. Un grand nombre de débats importants ont eu lieu au cours de l'année visée par le rapport.

Projet C-13 : nouvelle version sur l'« accès légal »

Un débat long et vigoureux a suivi la présentation du projet de loi C-13, Loi sur la protection des Canadiens contre la cybercriminalité, en novembre 2013.

Certains critiques ont qualifié le projet de loi C-13 de cheval de Troie. Rédigé à la suite des suicides très médiatisés de jeunes filles qui avaient été victimes de cyberintimidation, le projet de loi C-13 aurait pour effet de rendre illégale la distribution d'images intimes sans le consentement de la personne représentée, ainsi que d'éliminer les obstacles au retrait de ces images sur Internet.

Cependant, la loi proposée donnerait également à la police et à d'autres autorités de nouveaux outils pour conserver des registres sur l'utilisation d'ordinateurs et les transmissions électroniques, ainsi que suivre et localiser diverses activités en ligne de suspects; elle faciliterait l'approbation par les tribunaux de la surveillance électronique et élargirait l'accès légal d'un éventail plus grand d'organismes d'enquête.

Après le dépôt du projet de loi C-13 en novembre 2013, le Commissariat l'a analysé de manière approfondie, jusqu'à la comparution, le 10 juin 2014, du commissaire Daniel Therrien devant le Comité permanent de la justice et des droits de la personne de la Chambre des communes.

Dans sa déclaration, le commissaire a recommandé de scinder le projet de loi, c'estàdire de soumettre la partie sur la cyberintimidation au Parlement en vue d'une décision rapide, tout en permettant un examen précis et ciblé des dispositions sur l'accès légal. Il a résumé les quatre principales préoccupations du Commissariat :

- l'abaissement du seuil d'autorisation de l'accès par l'État aux renseignements personnels électroniques, passant de la norme actuelle de « motifs raisonnables et probables » à une nouvelle norme basée sur un « motif raisonnable de soupçonner » une activité illégale;

- la multiplication des autorités qui pourraient invoquer les nouveaux pouvoirs de surveillance, en plus des agents de police, notamment l'inclusion d'une catégorie mal définie de « fonctionnaires publics » comprenant les maires, les préfets, les agents des pêches, les agents des douanes et tout agent fédéral ou provincial;

- la garantie d'immunité juridique à une personne ou à une organisation qui communique volontairement des renseignements à un enquêteur sans l'autorisation d'un tribunal;

Projet de loi C-13 – Déclaration du commissaire : https://www.priv.gc.ca/parl/2014/parl_20140610_f.asp

Mémoire présenté au Comité : https://www.priv.gc.ca/parl/2014/parl_sub_140609_f.asp

- l'absence de régime de transparence exigeant l'établissement de rapports réguliers sur l'utilisation des nouveaux pouvoirs.

Une transcription de la déclaration du commissaire et un mémoire plus détaillé peuvent être consultés sur le site Web du Commissariat.

Le 13 juin, le Comité a fait rapport à la Chambre des communes au sujet du projet de loi C-13; aucune autre mesure n'a été prise avant le congé estival.

Obtenir des renseignements sur les salaires

Le Commissariat est depuis longtemps un fervent partisan du gouvernement ouvert comme moyen d'améliorer la transparence et la responsabilité, tout en tenant compte des lois sur la protection de la vie privée. Le 5 juin 2013, Jennifer Stoddart, alors commissaire, a réaffirmé cette position lors d'une comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

Le Comité étudiait alors le projet de loi C-461, Loi sur la communication de renseignements et la transparence de la SRC et de la fonction publique, un projet de loi émanant d'un député.

La loi aurait modifié la *Loi sur la protection des renseignements personnels* de sorte que les salaires des fonctionnaires fédéraux dont les traitements sont les plus élevés deviennent des renseignements « non personnels » susceptibles d'être divulgués en réponse à une demande présentée en application de la *Loi sur l'accès à l'information.* Il en aurait été de même des échelles de traitement de tous les autres fonctionnaires et des dépenses remboursées à tout employé fédéral.

Après examen des pratiques en cours à la fonction publique, aux gouvernements provinciaux et au secteur privé, la commissaire Stoddart a déclaré au Comité que « la divulgation des salaires des cadres supérieurs des niveaux les plus élevés de la fonction publique ne représente pas un risque important quant à la protection de la vie privée, par rapport à l'objectif de transparence et à l'intérêt général du public. »

La commissaire Stoddart a ajouté que la divulgation des échelles de traitement et des dépenses remboursées ne représente pas de risques graves au chapitre de la protection de la vie privée et que le Commissariat divulguerait facilement ces renseignements en réponse à une demande d'accès à l'information.

Le projet de loi C-416 est mort au feuilleton de la Chambre des communes en février 2014.

Les agents du Parlement unissent leurs efforts

L'importance d'améliorer la transparence et la responsabilité envers le Parlement et les Canadiens a également figuré dans les observations écrites présentées par la commissaire par intérim Chantal Bernier et six autres agents du Parlement désignés, dont le vérificateur général et le commissaire aux langues officielles.

Ces sept personnes, toutes nommées par le Parlement, ont commenté un projet de loi émanant d'un député, le projet de loi C-520,

Loi visant à soutenir l'impartialité politique des agents du Parlement.

Entre autres dispositions de la loi proposée, les candidats à un emploi dans les bureaux d'agents du Parlement seraient tenus de divulguer leur appartenance et leurs activités politiques des dix dernières années.

Le projet de loi prévoit également qu'un agent du Parlement, par exemple le commissaire à la protection de la vie privée, doit procéder à l'examen d'une allégation écrite d'un député ou d'un sénateur voulant qu'un employé d'un agent du Parlement ait manifesté une conduite partisane dans l'exercice de ses responsabilités. L'agent du Parlement serait tenu légalement de soumettre son rapport par écrit aux présidents du Sénat et de la Chambre des communes.

Lettre des agents du Parlement concernant le projet de loi C-520 : http://www.oic-ci.gc.ca/fra/activites-parlementaires-autres-documents-2014-other-parliamentary-documents_1.aspx

Dans une lettre adressée au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes, les sept agents, tout en soutenant les principes généraux de la responsabilité et de l'impartialité, ont critiqué le projet de loi C-520 au motif qu'il était trop large et trop vague, et incompatible avec les lois qui régissent actuellement l'emploi dans la fonction publique.

Le 26 mai, le Comité a fait rapport à la Chambre des communes sur le projet de loi C520, avec des modifications; aucune autre mesure n'a été prise avant le congé estival.

VÉRIFICATIONS DE LA CONFORMITÉ À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

En vertu de la *Loi sur la protection des renseignements personnels*, le commissaire peut vérifier les pratiques pertinentes en matière de protection des renseignements personnels des ministères et organismes fédéraux, et recommander des mesures correctrices au besoin. Même si la *Loi* ne prévoit pas de pouvoirs d'application, le commissaire peut publier ses conclusions et ses recommandations.

Habituellement, le Commissariat fait un suivi auprès des institutions deux ans après qu'elles ont été soumises à une vérification, en leur demandant quelles mesures elles ont prises pour donner suite à ses recommandations. En 2013-2014, nous avons lancé deux nouvelles vérifications et procédé au suivi de deux autres.

Suivis : En 2011, nous avons vérifié deux bases de données de la GRC : une base de données contenant des renseignements sur les crimes et les criminels, que peuvent extraire les services de police à l'échelle du Canada, et une constituant le principal système de gestion des dossiers opérationnels de la GRC. La description de la vérification et les recommandations se trouvent sur le site Web du Commissariat.

Rapport de vérification de certaines bases de données opérationnelles de la GRC 2011 : https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_rcmp_2011_f.asp

La GRC nous a avisés que quatre de nos six recommandations avaient été pleinement mises en œuvre et que les deux autres l'étaient en grande partie. Par exemple, pour résoudre le problème de la conservation plus longue que nécessaire de renseignements personnels dans le système de gestion des dossiers, la GRC nous a informés qu'elle avait éliminé l'arriéré de tous les dossiers en suspens et qu'elle efface maintenant les fichiers chaque jour conformément aux exigences. La GRC nous a également indiqué que tous les services de police, sauf ceux du Québec où la loi provinciale interdit aux services de police de conclure individuellement des ententes avec des organismes fédéraux, ont à présent signé des protocoles d'entente officiels contenant des dispositions sur la protection des renseignements personnels contenus dans la base de données sur les crimes et les criminels.

Protection de la vie privée et sécurité aérienne : Examen de l'Administration canadienne de la sûreté du transport aérien 2011 : https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_catsa_2011_f.asp

En 2011, nous avons également examiné les politiques et les pratiques de protection des renseignements personnels de l'Administration canadienne de la sûreté du transport aérien (ACSTA), une organisation connue de tous les passagers aériens. L'information peut être consultée sur notre site Web.

L'ACSTA nous a avisés que dix de nos douze recommandations ont été pleinement mises en œuvre, et les deux autres, en grande partie, notamment :

- ne plus avertir la police si des passagers d'un vol intérieur transportent avec eux d'importantes sommes d'argent;
- préparer un dépliant pour expliquer la manière dont l'ACSTA recueille, utilise, divulgue, conserve et élimine les renseignements personnels relativement aux cartes d'embarquement;
- implanter un nouveau logiciel en 2013-2014 pour illustrer à l'aide d'une figure générique une fouille effectuée avec un scanneur corporel au lieu d'une silhouette.

Nouvelles vérifications : Bien que les dispositifs de stockage portatifs tels que les clés USB et les disques durs externes puissent être d'usage souple et pratique, ils peuvent présenter des risques inhérents pour la sécurité et la protection des renseignements personnels, comme a pu s'en rendre compte un ministère fédéral comme Emploi et Développement social Canada.

Pour en savoir plus sur l'utilisation des dispositifs de stockage portatifs dans les institutions fédérales, le Commissariat a effectué un sondage auprès des ministères et des organismes, et a retenu 17 d'entre eux en vue d'un examen plus approfondi dans le cadre d'une vérification à l'échelle du gouvernement. La vérification permettra d'évaluer si ces institutions ont établi et mis en œuvre des politiques, des procédures et des mesures adéquates pour protéger les renseignements personnels stockés sur ces dispositifs. Nous comptons terminer cette vérification en 2014-2015.

Le Commissariat a également lancé un examen des demandes d'accès sans mandat aux renseignements de base sur les abonnés qu'adresse la GRC aux compagnies de télécommunications et aux fournisseurs de

Rapport de vérification 2013 de l'ARC : https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_cra_2013_f.asp

services Internet. Cet examen, et les résultats, sont présentés en détail à la section 4 du présent rapport.

Diffusion : En 2013-2014, le Commissariat a publié ses vérifications officielles de l'Agence du revenu du Canada et du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), qui ont été l'une et l'autre présentées dans le rapport annuel de l'an dernier.

ENQUÊTES

Un examen attentif des chiffres montre que le Commissariat à la protection de la vie privée tire encore profit des mesures mises en place dans les années précédentes qui visaient à traiter plus efficacement les plaintes. Malgré des plaintes de plus en plus nombreuses et complexes, le Commissariat a continué de constater une amélioration au chapitre du délai de traitement.

Rapport de vérification 2013 du CANAFE : https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_2013_f.asp

En 2013-2014, le Commissariat a accepté 1 777 plaintes en vertu de *la Loi sur la protection des renseignements personnels*, donc beaucoup moins que lors de l'exercice précédent. Mais en 2012-2013, le nombre de plaintes reçues était anormalement élevé puisque plus de 1 200 plaintes étaient attribuables à deux atteintes graves à la protection des données à Emploi et Développement social Canada (EDSC). En soustrayant le nombre de plaintes liées à ces deux atteintes du total des plaintes reçues en 20122013, on constate tout de même une augmentation d'environ 700 plaintes en 2013-2014.

En 2013-2014, le délai de traitement moyen des plaintes a été de 10,9 mois. Si l'on exclut les plaintes relatives à EDSC, on constate que le délai de traitement s'est amélioré, passant de 8,9 mois en 2012-2013 à 8,1 en 2013-2014.

Cela représente une nette amélioration comparativement à il y a cinq ans, soit en 2008-2009, où la moyenne était de 19,47 mois. Année après année, les tendances indiquent que les plaintes augmentent en volume et en complexité. Dans ce contexte, le délai de traitement moyen a continué de s'améliorer graduellement de façon générale, grâce aux efforts visant la redistribution des ressources internes ainsi que l'amélioration et la modernisation des processus.

Par exemple, le processus de règlement rapide a permis de clore 345 de nos dossiers, comparativement à 299 en 2012-2013. En plus de gérer davantage de plaintes par cette méthode de négociation et de conciliation cette année, le Commissariat est parvenu à réduire de quatre jours le délai de traitement moyen des cas de règlement rapide (de 2,25 mois à 2,11 mois, comme le montrent les tableaux détaillés qui se trouvent à l'annexe 2).

Les cinq enquêtes ci-après présentent un intérêt particulier.

La perte de la clé USB d'Emploi et Développement social Canada confirme les leçons tirées

Une enquête antérieure, relative à une atteinte à la protection des données concernant EDSC, a été présentée dans un rapport spécial du Commissariat qui a été déposé au Parlement le 25 mars 2014. Il y était souligné que les politiques officielles de protection des renseignements personnels et de sécurité des données de l'organisation ne se traduisaient pas par des pratiques opérationnelles valables.

À l'issue de son enquête, le Commissariat a conclu que ce facteur a largement contribué à la perte d'un disque dur contenant les renseignements personnels de 583 000 bénéficiaires de prêts étudiants, disque dur dont l'absence a été constatée le 5 novembre 2012.

Le même mois, une clé USB contenant les renseignements personnels de 5 045 particuliers ayant interjeté appel de décisions relatives à des prestations d'invalidité du Régime de pensions du Canada a disparu du bureau de travail d'un employé dans un local d'EDSC. Comme le disque dur, la clé USB n'était ni protégée par un mot de passe ni chiffrée, et elle n'a jamais été retrouvée.

Les renseignements personnels suivants étaient notamment stockés sur la clé USB disparue, pour chaque personne : NAS, date de naissance, nom, état de santé, niveau de scolarité, type d'emploi; l'information indiquait également si d'autres paiements étaient versés, par exemple des indemnités d'accident du travail. Si des renseignements de ce type tombent entre de mauvaises mains, cela peut donner lieu au vol d'identité ou à la fraude.

L'enquête menée par le Commissariat sur la disparition de la clé USB a mis au jour des lacunes dans les quatre mêmes types de contrôles de gestion de la protection des renseignements personnels examinés dans le cas du disque dur contenant des renseignements sur les prêts étudiants, à savoir les contrôles physiques, technologiques et administratifs, et les contrôles du personnel.

La différence entre le cas de la disparition de la clé USB et le cas du disque dur (contenant les renseignements personnels des bénéficiaires de prêts étudiants) réside dans le fait que c'est un avocat de Justice Canada qui avait la garde de la clé USB lorsqu'elle a été perdue. L'avocat travaillait dans un bureau d'EDSC pour aider au triage des appels interjetés d'une décision relative aux pensions d'invalidité en attente d'audition devant l'ancien tribunal de révision. L'avocat a laissé la clé USB sur le bureau dans une pièce fermée au lieu de ranger la clé dans un classeur sécurisé.

De façon plus générale, notre enquête a montré que le ministère de la Justice n'a pas non plus concrétisé ses politiques de sécurité et de protection des renseignements personnels dans des pratiques opérationnelles efficaces.

EDSC et Justice ont accepté les neuf recommandations du Commissariat visant à mieux protéger les renseignements personnels dont ils ont la garde. La plupart de ces recommandations reprennent celles formulées lors de l'enquête sur la perte du disque dur.

Personnes recherchées dans le cadre du programme de l'ASFC

Dans une plainte déposée au Commissariat, le Conseil canadien pour les réfugiés a allégué que les renseignements personnels d'une personne avaient été divulgués de façon indue sur le site Web de l'Agence des services frontaliers du Canada (ASFC). Cette divulgation a été faite dans le cadre du programme des « personnes recherchées par l'ASFC », où l'on demande l'aide de la population pour retrouver des personnes faisant l'objet de mandats de renvoi actif pancanadien. L'homme en question faisait partie des 30 personnes décrites comme étant des personnes « accusées, ou complices, de crimes de guerre et de crimes contre l'humanité ».

Le site Web du programme fournissait les noms, les dates de naissance et les photographies de toutes les personnes, au nombre de trente. Malgré le fait que le programme touchait des renseignements personnels, l'ASFC n'a pas procédé à une EFVP. Cette lacune présentait des risques graves sur le plan de la protection de la vie privée parce que les conséquences pour les personnes citées dans le programme pouvaient être lourdes.

Dans son enquête, le Commissariat a conclu que la divulgation des renseignements personnels de cette personne était permise aux termes de la *Loi sur la protection des renseignements personnels* dans la mesure où le motif de la divulgation est conforme à l'administration et à l'application de la loi sur l'immigration et, de ce fait, un usage cohérent avec la *Loi*.

Toutefois, l'Agence n'a pas pris toutes les mesures raisonnables pour s'assurer que les renseignements personnels étaient aussi exacts, à jour et complets que possible, comme l'exige également la *Loi sur la protection des renseignements personnels*. Par exemple, dans ce cas, la personne n'avait pas été reconnue coupable de crimes de guerre sous le régime du droit criminel, mais plutôt déclarée interdite de territoire en vertu de la loi et des règlements de l'immigration du Canada à titre de fonctionnaire d'un gouvernement non identifié, soupçonné de commettre des crimes de guerre.

Par conséquent, cet aspect de la plainte a été jugé fondé.

Comme suite à l'enquête du Commissariat, l'ASFC a accepté intégralement ses cinq recommandations.

L'ASFC s'est engagée à prendre les mesures suivantes :

- modifier la quantité de renseignements personnels divulgués dans le cadre du programme, notamment en les retirant tous, sauf la photographie, le nom et le statut, lorsque la personne est retrouvée ou expulsée du Canada; bien que notre enquête ait mené à la conclusion que la divulgation de renseignements personnels était nécessaire pour atteindre l'objectif du programme, nous n'étions pas convaincus que l'ASFC limitait de façon adéquate la quantité de données nécessaires à cette fin. Par exemple, l'ASFC n'a fourni aucune justification concernant la divulgation complète de la date de naissance des individus;

- dans les prochaines lettres d'avis transmises au Commissariat conformément au paragraphe 8(5), démontrer en quoi des raisons d'intérêt public justifieraient nettement une violation de la vie privée qui pourrait résulter d'un cas particulier, et indiquer quels renseignements seront divulgués, comment et pendant combien de temps ils seront accessibles au public.

- indiquer clairement sur le site Web la différence entre un verdict de culpabilité sous le régime du droit criminel et une décision en vertu des lois sur l'immigration;

- mieux faire appliquer sa pratique de supprimer les profils du site Web dans les 30 jours qui suivent l'arrestation d'une personne ou son renvoi du Canada, contrairement à ce qui s'est produit dans ce cas, où le profil de la personne est resté affiché au moins six mois après son arrestation;

- modifier le fichier de renseignements personnels pertinent pour rendre compte des usages compatibles des renseignements personnels dans le cadre du programme;

Depuis, l'ASFC a avisé le Commissariat qu'elle en est à l'étape de planification de cette EFVP, qui devrait être achevée à l'automne 2014.

Une femme ne parvient pas à remettre des renseignements personnels à l'Agence du revenu du Canada

Lorsqu'une femme de la Colombie-Britannique a tenté de remettre des renseignements personnels d'autres contribuables, qui lui avaient été envoyés par erreur, l'Agence du revenu du Canada (ARC) n'a agi qu'une fois que les médias ont été informés de l'affaire.

Tout a commencé lorsque cette résidente de la Colombie-Britannique a demandé à l'ARC, à la fin du mois de mars 2013, les renseignements nécessaires pour remplir la déclaration de revenus de sa fille décédée. Environ huit semaines après, elle recevait un épais colis du Centre fiscal de Surrey.

Le colis contenait non seulement les feuillets de renseignements pour la déclaration de revenus de sa fille, mais également les renseignements personnels confidentiels, tels que le nom, le revenu et les prestations, le NAS, la date de naissance, la situation de famille, les données d'emploi, de cinq autres personnes qui lui étaient inconnues.

Dans une entrevue au réseau anglais de RadioCanada, la femme a expliqué qu'elle a tenté à plusieurs reprises de signaler cette atteinte en composant le numéro d'appel gratuit de l'ARC, mais qu'elle n'a pu parler à personne. (L'ARC indique que l'objectif en matière d'accessibilité des appelants pour les demandes de renseignements généraux est de 85 %, ce qui signifie que l'Agence reconnaît qu'un appelant sur sept ne pouvait joindre le service.)

La femme a ensuite essayé de remettre les documents confidentiels en personne en se rendant en voiture jusqu'au Centre fiscal de Surrey, qui n'était pas ouvert au public. Un gardien de sécurité lui a suggéré de placer le colis non scellé et non étiqueté contenant les renseignements personnels confidentiels dans une boîte de dépôt située à l'extérieur de l'immeuble.

Cette suggestion ne lui semblant pas convenir, la femme a de nouveau téléphoné, de sa voiture, au numéro principal de l'ARC. On lui a répondu qu'elle pouvait placer les documents dans une autre enveloppe scellée indiquant la désignation de sécurité appropriée et glisser l'enveloppe dans la boîte de dépôt, ou bien attendre 10 jours que l'ARC lui envoie une enveloppe spécialement étiquetée.

Insatisfaite de ce qui lui était proposé, la femme a suggéré de remettre en main propre les documents à un employé du centre fiscal, mais on lui a répondu que c'était impossible.

C'est alors qu'elle a décidé de communiquer avec un journaliste du réseau anglais de RadioCanada, qui a pris contact avec l'ARC. Le jour suivant, un employé du bureau des services fiscaux de la Colombie-Britannique est venu chercher les documents des contribuables au domicile de la femme.

Dans un rapport, l'ARC a confirmé les principales circonstances de l'incident. Lorsqu'il a été mis au courant, le Commissariat a déposé une plainte. Notre enquête a permis de conclure que l'ARC a porté atteinte au droit à la vie privée des contribuables et que la plainte était fondée.

L'ARC s'est engagée à prendre des mesures correctives pour réduire le risque de répétition d'incidents semblables, y compris en proposant d'envoyer par service de messagerie des enveloppes affranchies.

L'ARC a maintenant amélioré ses procédures internes concernant les services à la clientèle et le courrier mal acheminé. Si le Commissariat est satisfait des mesures, il aurait aimé que l'ARC en prenne d'autres pour faciliter encore le signalement par le public des atteintes à la sécurité des renseignements personnels, en particulier aux périodes de pointe.

La durée de conservation des dossiers disciplinaire par la GRC est contestée

L'arrêt *R. c. McNeil* de la Cour suprême du Canada a créé l'obligation pour la Couronne de divulguer à l'avocat de la défense les dossiers touchant des constatations d'inconduite grave de la part d'agents de police chargés d'enquêtes, dans les cas où les dossiers sont pertinents pour la poursuite intentée contre un accusé.

Un représentant des relations de travail a déposé une plainte au Commissariat au nom de membres de la GRC. Dans sa plainte, il affirmait que la divulgation à la Couronne des dossiers disciplinaires non officiels n'était pas compatible avec l'arrêt *McNeil,* soutenant que la Cour suprême exige la divulgation de dossiers disciplinaires uniquement dans les cas où l'inconduite alléguée a fait l'objet d'une audience.

La GRC est d'avis que les problèmes d'inconduite de gravité variable par des policiers peuvent être traités par des procédures disciplinaires officielles ou non, de sorte que l'exclusion de tous les dossiers en lien avec des procédures disciplinaires non officielles pourrait contrevenir à l'arrêt *McNeil* du fait que cela pourrait empêcher la Couronne, ainsi que l'avocat de la défense, d'avoir accès à des dossiers qui pourraient présenter un intérêt.

Nous avons exprimé notre accord avec cette position, et nous avons insisté sur le fait qu'il appartient à la Couronne de juger de la pertinence des dossiers disciplinaires dans une procédure donnée.

Même si nous avons jugé la plainte non fondée, nous avons été très préoccupés par les politiques de conservation qu'applique la GRC aux dossiers disciplinaires. En effet, ces dossiers sont conservés jusqu'à ce que chaque membre de la GRC soit âgé de 100 ans, alors que la plupart des services de police du pays ne conservent l'information de nature disciplinaire ou les renseignements sur les inconduites que pour une période de trois à cinq ans. Nous avons donc recommandé que la GRC réexamine ses politiques de conservation. Depuis, la GRC a répondu qu'elle maintiendrait la pratique actuelle.

Les délais suscitent toujours des préoccupations

Dans le rapport annuel de l'an dernier, nous avions noté que les plaintes relatives aux délais n'ont cessé d'augmenter ces dernières années, et nous en avons reçu un nombre record en 2012-2013, soit 437 au total. En 2013-2014, il semble que les institutions fédérales éprouvent toujours de la difficulté à honorer leurs obligations, puisque ce chiffre est passé à 585.

Comme c'était le cas au cours des années précédentes, Service correctionnel Canada est l'organisation visée par le plus grand nombre de plaintes touchant les délais, soit 296 au total.

De nombreuses organisations ont fait connaître les difficultés qu'elles avaient à respecter les délais en raison d'un manque de ressources ou de problèmes de traitement des demandes pour lesquelles il faut une vaste gamme de documents.

Au cours de l'année, nous avons poursuivi le travail avec les ministères, en leur demandant des plans d'action qui donnent des dates d'engagement claires pour la réponse aux demandes présentées par des particuliers au sujet de leurs renseignements personnels.

L'École de la fonction publique appelée à mieux protéger la confidentialité

Des cadres supérieurs de l'École de la fonction publique, principal établissement de formation du gouvernement fédéral, ont fait l'expérience directe de la nécessité de disposer de procédures de protection des renseignements personnels.

En août 2012, l'École a reçu une lettre du commissaire à l'intégrité du secteur public, le fonctionnaire fédéral chargé de surveiller l'application de la loi canadienne sur les dénonciateurs, la *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles.*

La lettre avisait l'École que le commissaire à l'intégrité du secteur public allait faire enquête sur de nombreuses allégations d'inconduite contre sept employés de l'École, en nommant les sept personnes et les actes répréhensibles allégués.

L'École a fait remettre une copie de la lettre du Commissariat à l'intégrité en main propre à chacun des sept employés nommés comme auteurs présumés des actes répréhensibles, les avisant de coopérer pleinement à l'enquête.

L'un des sept employés faisant l'objet d'une enquête s'est également plaint au Commissariat à la protection de la vie privée que ses renseignements personnels, en raison de la révélation de son nom dans la lettre susmentionnée, avaient été rendus publics en contravention des dispositions de la *Loi sur la protection des renseignements personnels*. Nous avons conclu, à l'issue de notre enquête, que cette plainte était fondée.

À la suite des recommandations du Commissariat, l'École a mis en place des procédures pour assurer la confidentialité des renseignements associés à la *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles,* et un plan pour gérer les atteintes à la sécurité des renseignements personnels.

ANNEXE 1 – Définitions

Types de plaintes généraux

1. Accès

Accès — Tous les renseignements personnels n'auraient 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'aurait pas apporté les corrections aux renseignements personnels ou ne les aurait pas annotés parce qu'elle n'approuve pas les corrections demandées.

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

Frais — Des frais auraient 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 décrirait pas de façon adéquate le fonds de renseignements personnels d'une institution.

2. Protection des renseignements personnels

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

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

Conservation et retrait — Des renseignements personnels n'auraient pas été conservés selon les calendriers de conservation et de retrait approuvés par les Archives nationales et publiés dans *Info Source* : ils 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 auraient été 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'aurait pas répondu dans les délais prescrits.

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

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

Conclusions générales 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 où 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.

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 pouvoir être joint pour fournir des renseignements supplémentaires essentiels pour arriver à une conclusion.

2. Autres décisions

Réglée rapidement : S'applique aux cas où l'affaire est réglée avant même qu'une enquête régulière 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 jugé 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 régulière 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 ».

ANNEXE 2 – Tableaux statistiques

Plaintes et enquêtes en vertu de la Loi sur la protection des renseignements personnels, du 1er avril 2013 au 31 mars 2014

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* en 2013-2014

Catégorie	Total
Acceptées	
Accès	515
Délais	585
Protection des renseignements personnels	677
Total	**1 777**
Fermées à la suite d'une enquête en vue d'un règlement rapide	
Accès	148
Délais	101
Protection des renseignements personnels	96
Total	**345**
Fermées au moyen du processus d'enquête officiel	
Accès	255
Délais	446
Protection des renseignements personnels	1 039
Total	**1 740**
Total des plaintes fermées	**2 085**
Atteintes signalées	
Divulgation accidentelle	154
Vol	9
Perte	29
Accès non autorisé	36
Total des plaintes reçues	**228**

Atteintes à la *Loi sur la protection des renseignements personnels*, par institution

Mis en cause	Incident
Anciens Combattants Canada	60
Citoyenneté et Immigration Canada	54
Agence du revenu du Canada	33
Service correctionnel Canada	22
Ministère des Affaires étrangères, du Commerce et du Développement	9
Gendarmerie royale du Canada	9
Pêches et Océans	6
Affaires autochtones et Développement du Nord Canada	4
Statistique Canada	4
Justice Canada	2
Agence des services frontaliers du Canada	2
Exportation et développement Canada	2
Ressources naturelles Canada	2
Bureau de l'ombudsman de l'approvisionnement	1
Patrimoine canadien	1
Conseil des arts du Canada	1
Commission canadienne des droits de la personne	1
Secrétariat du Conseil du Trésor du Canada	1
Agence de promotion économique du Canada atlantique	1
Travaux publics et Services gouvernementaux Canada	1
Centre de la sécurité des télécommunications	1
Services partagés Canada	1
Agriculture et Agroalimentaire Canada	1
Transports Canada	1
Emploi et Développement social Canada	1
Société canadienne des postes	1
Agence canadienne d'inspection des aliments	1
Environnement Canada	1
Sécurité publique Canada	1
Commission de la fonction publique du Canada	1
Commission des libérations conditionnelles	1
Services des poursuites pénales du Canada	1
Grand Total	**228**

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

Mis en cause	Fondée	Fondée - Résolue	Non fondée	Résolue	Réglée rapidement - Résolue	Abandonnée	Hors du champ d'application	Réglée en cours d'enquête	Grand Total
Affaires autochtones et Développement du Nord Canada	2	2	3	1	1	5	0	1	**15**
Banque du Canada	0	0	0	0	2	0	0	0	**2**
Agence des services frontaliers du Canada	2	2	11	1	4	9	0	1	**30**
Développement économique Canada pour les régions du Québec	0	0	0	0	0	0	0	1	**1**
Centre des armes à feu du Canada	0	0	0	0	1	0	0	0	**1**
Société canadienne des postes	2	2	2	1	7	0	0	0	**14**
Agence du revenu du Canada	3	1	20	1	14	5	1	1	**46**
École de la fonction publique du Canada	1	0	0	0	1	0	0	0	**2**
Société Radio-Canada	0	0	0	0	1	0	0	0	**1**
Agence canadienne d'inspection des aliments	0	0	3	4	0	0	0	0	**7**
Patrimoine canadien	0	0	0	1	0	0	0	0	**1**
Commission canadienne des droits de la personne	0	1	1	0	1	0	0	0	**3**
Tribunal canadien des droits de la personne	0	0	0	0	0	0	0	1	**1**
Musée canadien des civilisations	0	1	0	0	0	0	0	0	**1**
Service canadien du renseignement de sécurité	0	1	11	0	0	1	0	0	**13**
Citoyenneté et Immigration Canada	2	1	2	1	11	14	0	1	**32**
Service correctionnel Canada	15	2	29	3	97	30	0	9	**185**
Élections Canada	1	0	1	0	1	0	0	0	**3**
Environnement Canada	0	1	0	1	0	0	0	0	**2**
Pêches et Océans	0	0	1	0	8	2	0	0	**11**
Santé Canada	2	0	0	0	4	1	0	2	**9**
Commission de l'immigration et du statut de réfugié du Canada	0	1	0	0	5	0	0	0	**6**

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

Mis en cause	Fondée	Fondée – Résolue	Non fondée	Résolue	Réglée rapidement – Résolue	Abandonnée	Hors du champ d'application	Réglée en cours d'enquête	Grand Total
Industrie Canada	0	0	1	0	0	0	0	1	**2**
Justice Canada	1	3	5	0	3	4	0	1	**17**
Bibliothèque et Archives Canada	0	0	0	0	1	0	0	0	**1**
Musée des beaux-arts du Canada	0	1	0	0	0	0	0	0	**1**
Ressources naturelles Canada	0	0	0	0	3	0	0	0	**3**
Conseil de recherches en sciences naturelles et en génie du Canada	1	0	0	0	0	0	0	0	**1**
Bureau de l'enquêteur correctionnel	0	0	2	0	0	0	0	0	**2**
Commissariat à l'information du Canada	0	0	0	0	0	1	0	0	**1**
Parcs Canada	0	0	0	0	2	0	0	0	**2**
Commission des libérations conditionnelles	0	0	2	0	2	0	0	0	**4**
Passeport Canada	11	0	0	0	7	2	0	0	**20**
Agence de la santé publique du Canada	0	0	0	0	0	3	0	0	**3**
Services des poursuites pénales du Canada	0	0	2	0	0	0	0	0	**2**
Sécurité publique Canada	0	0	0	0	2	0	0	0	**2**
Intégrité du secteur public du Canada	0	0	0	0	0	1	0	0	**1**
Tribunal de la dotation de la fonction publique	0	0	1	0	0	0	0	0	**1**
Travaux publics et Services gouvernementaux Canada	2	0	2	0	2	2	0	0	**8**
Monnaie royale canadienne	0	0	1	0	1	0	0	0	**2**
Gendarmerie royale du Canada	7	14	20	4	26	5	0	5	**81**
Comité d'examen externe de la Gendarmerie royale du Canada	0	0	1	0	0	0	0	0	**1**
Comité de surveillance des activités de renseignement de sécurité	0	1	0	0	0	0	0	0	**1**
Services partagés Canada	0	0	0	0	1	0	0	1	**2**

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

Mis en cause	Fondée	Fondée - Résolue	Non fondée	Résolue	Réglée rapidement - Résolue	Abandonnée	Hors du champ d'application	Réglée en cours d'enquête	Grand Total
Conseil de recherches en sciences humaines du Canada	1	0	0	0	0	0	0	0	**1**
Statistique Canada	0	1	16	0	3	1	0	0	**21**
Transports Canada	1	1	1	0	3	0	0	10	**16**
Bureau de la sécurité des transports du Canada	1	0	0	0	0	0	0	0	**1**
Secrétariat du Conseil du Trésor du Canada	0	0	1	0	0	0	0	0	**1**
Anciens Combattants Canada	6	1	5	1	2	0	0	0	**15**
Service Canada	0	0	0	0	4	0	0	2	**6**
Ministère des Affaires étrangères, du Commerce et du Développement	1	1	0	0	0	1	0	2	**5**
Emploi et Développement social Canada	872	0	3	0	16	7	0	0	**898**
Ministère de la Défense nationale	1	2	8	3	8	3	2	2	**29**
Commission de la fonction publique du Canada	0	1	0	0	0	0	0	0	**1**
Grand Total	**935**	**41**	**155**	**22**	**244**	**97**	**3**	**41**	**1538**

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

Type de plainte	Nombre	Délai de traitement moyen (en mois)
Accès		
Accès	143	2,17
Correction/annotation	4	1,20
Refus d'accès	1	0,16
Délais		
Délais	97	1,97
Correction/délais	3	3,01
Avis de prorogation	1	1,67
Protection des renseignements personnels		
Utilisation et communication	74	2,46
Collecte	18	1,42
Conservation et retrait	3	1,15
Politique	1	0,23
Total	**345**	**2,11**

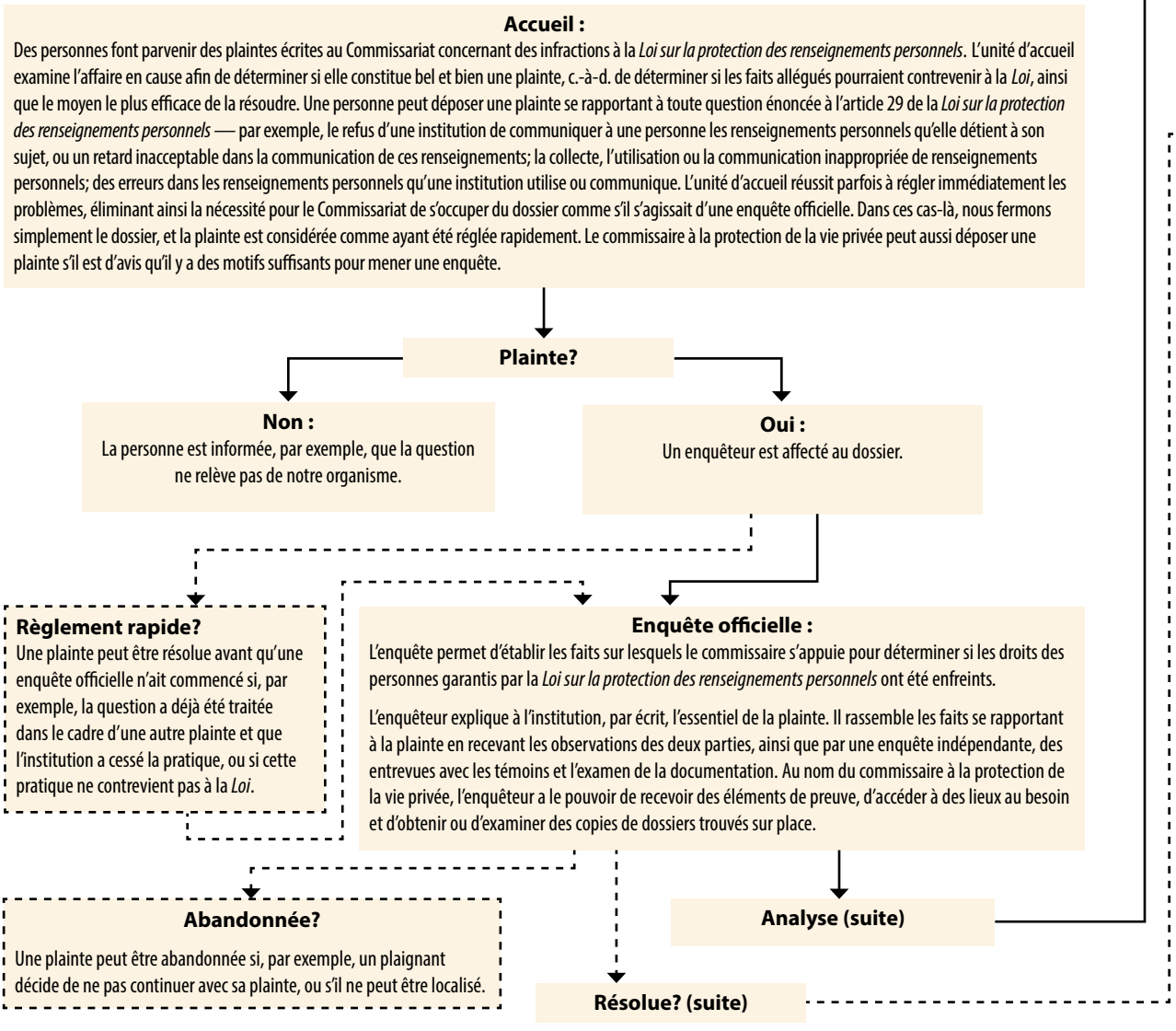
Délais de traitement des plaintes en vertu de la *Loi sur la protection des renseignements personnels* — Enquêtes officielles, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen (en mois)
Accès		
Accès	253	11,29
Correction/annotation	2	1,61
Délais		
Délais	433	4,52
Avis de prorogation	11	4,81
Correction/délais	2	5,39
Protection des renseignements personnels		
Utilisation et communication	1 024	13,59
Collecte	10	10,12
Conservation et retrait	5	8,20
Total	**1 740**	**10,87**

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

Type de plainte	Nombre	Délai de traitement moyen (en mois)
Plaintes officielles		
Fondée	1 318	11,13
Non fondée	193	10,56
Abandonnée	118	6,66
Fondée et résolue	42	18,25
Réglée en cours d'enquête	41	8,40
Résolue	25	13,01
Hors du champ d'application	5	3,29
Réglée rapidement et résolue	343	2,11
Total	**2 085**	**9,43**

ANNEXE 3 – Processus d'enquête



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

Analyse :

L'enquêteur analyse les faits et prépare les recommandations pour le 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 au 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*. Le 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 :

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

Le commissaire 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 le commissaire ou son délégué, ainsi que toute recommandation faite à l'institution. Le 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 au 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, le 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 le commissaire à la protection de la vie privée, peut choisir de demander une audience à la Cour fédérale. La Cour fédérale a le pouvoir d'examiner l'affaire et de déterminer si l'institution doit fournir les renseignements au requérant.

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

ANNEXE 4 – Rapport 2013-2014 du commissaire spécial à la protection de la vie privée

Depuis le 1er avril 2007, le Commissariat à la protection de la vie privée est assujetti à la *Loi sur la protection des renseignements personnels*. La loi qui a donné lieu à cette modification n'a pas créé en même temps de mécanisme distinct pour enquêter sur les plaintes de traitement incorrect d'une demande d'accès au Commissariat.

Étant donné que l'examen indépendant des décisions visant la divulgation de l'information gouvernementale constitue un principe fondamental de l'accès à l'information, on a créé la fonction de commissaire spécial indépendant à la protection de la vie privée et on lui a conféré le pouvoir d'enquêter sur les plaintes déposées contre le Commissariat.

Plus précisément, en vertu du paragraphe 59(1) de la *Loi sur la protection des renseignements personnels*, le commissaire à la protection de la vie privée du Canada m'a délégué, en qualité de commissaire spécial à la protection de la vie privée :

Tous les pouvoirs et fonctions qui lui sont conférés aux termes des articles 29 à 35 et de l'article 42 de la *Loi*, sous réserve des restrictions et limites suivantes :

Conformément à l'alinéa 59(2)*a*), le commissaire investi de la délégation de pouvoirs ne peut procéder à des enquêtes portant sur les cas où le refus de communication de renseignements personnels est lié aux alinéas 19(1)*a*) or *b*) ou à l'article 21 de la *Loi.*

Je suis la quatrième personne à occuper cette fonction depuis 2007. C'est la première fois que je contribue au Rapport annuel du commissaire à la protection de la vie privée.

Cinq nouvelles plaintes ont été reçues et fait l'objet d'une enquête cette année. Trois ont fait l'objet d'une décision avant le 31 mars 2014. Les deux autres enquêtes étaient encore en suspens à cette date, mais elles ont été achevées peu de temps après la fin de la période de rapport.

Dans la première plainte, il s'agissait de déterminer si le Commissariat avait agi ou non assez rapidement au moment où il a voulu prolonger le délai de réponse à un demandeur. Les institutions sont tenues de répondre dans un délai de 30 jours, sauf si elles prolongent le délai de réponse pour des motifs valables, en en informant la personne concernée dans les 30 jours. Le Commissariat a envoyé par la poste l'avis le 28e jour, et l'avis est parvenu à l'adresse du plaignant le 35e jour. Dans ce cas, il fallait déterminer si l'envoi d'un avis écrit par le responsable de l'institution respectait cette exigence ou si la personne qui présente la demande doit réellement recevoir l'avis dans les 30 jours. Après avoir examiné le régime législatif, il a été conclu que l'obligation d'envoi de l'avis dans les 30 jours avait été honorée par le responsable de l'institution. Par conséquent, il a été déterminé que cette plainte était **non fondée.**

Dans une seconde plainte, présentée par la même personne, la question était de savoir si le Commissariat avait eu des motifs valables de prolonger le délai de réponse à la demande. Dans ce cas, le volet pertinent du critère selon la *Loi sur la protection des renseignements personnels* consistait à déterminer si le respect du délai initial « entraverait de façon sérieuse le fonctionnement de l'institution ». L'enquête a montré que le Commissariat a dû examiner un nombre exceptionnellement élevé de documents, environ 100 fois plus que pour une demande moyenne, et qu'il aurait été déraisonnable de demander

à un analyste d'étudier un si grand nombre de pages en 30 jours. Le Commissariat a affecté d'autres ressources à la tâche, pour pouvoir la terminer même avec la prorogation du délai. La plainte a également été jugée **non fondée.**

Dans la troisième plainte qui était reliée aux autres et émanait de la même personne, la principale allégation était que le Commissariat n'avait pas respecté ses obligations en vertu de la *Loi sur la protection des renseignements personnels* parce qu'il n'avait pas fait de recherche de courriels et de pièces jointes dans les « bandes de sauvegarde ». Les systèmes de sauvegarde sont conçus pour la protection des données (par exemple contre la suppression accidentelle de données, l'incendie ou les pannes de système). Ils ne constituent pas un système d'archives comportant une capacité de recherche et d'extraction rapides. Après enquête, nous avons conclu que la recherche d'informations sur les bandes de sauvegarde est toujours compliquée. Dans ce cas particulier, la complexité était plus grande encore parce que le demandeur n'a pas fourni d'« indications suffisamment précises pour que [le Commissariat] puisse retrouver [les renseignements] sans problèmes sérieux ». Il a également été déterminé que cette plainte était **non fondée.**

La principale question, dans chacune des deux dernières plaintes, concernait l'application en bonne et due forme de l'article 22.1 de la *Loi sur la protection des renseignements personnels*, qui prévoit une exception obligatoire dans certaines circonstances relatives à l'information obtenue ou créée par le Commissariat au cours d'une enquête. Une grande partie du travail lié à ces enquêtes a été fait, mais il n'était pas terminé en 2013-2014. Le prochain rapport annuel fera état de la conclusion définitive.

En plus de ces trois plaintes, le commissaire spécial a également reçu une plainte déposée par une personne insatisfaite de la façon dont le Commissariat a fait enquête sur sa plainte relative au traitement de ses renseignements personnels par un autre ministère. Le commissaire spécial n'est pas habilité à enquêter sur ce type de plaintes. Notre mandat se limite à recevoir des plaintes selon lesquels le Commissariat aurait mal géré lui-même les renseignements personnels dont il a la garde, et à faire enquête sur ces plaintes.

La fonction de commissaire spécial indépendant à la protection de la vie privée a été conçue pour assurer l'intégrité du processus lié aux plaintes, un élément essentiel de tout régime d'accès à l'information. Nous demeurons déterminés à enquêter de façon rigoureuse et indépendante sur les plaintes ultérieures déposées contre le Commissariat.

C'est un privilège d'assumer les fonctions de commissaire spécial à la protection de la vie privée.

Le tout respectueusement soumis,

John H, Sims, c.r.