Commissariat
à la protection de
la vie privée du Canada

Loi sur la protection des renseignements personnels

Rapport annuel au Parlement

2010-2011

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

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

Suivez-nous sur Twitter : @privacyprivee

N° de cat. IP50-2011F-PDF
ISBN 978-1-100-96575-8

Cette publication se trouve également au www.priv.gc.ca.

Commissaire à la protection de la vie privée du Canada

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

Privacy Commissioner of Canada

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

Novembre 2011

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 sur la *Loi sur la protection des renseignements personnels* pour la période du 1er avril 2010 au 31 mars 2011, conformément à l'article 38 de la *Loi*.

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

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

(Original signé par)

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada

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

Privacy Commissioner of Canada

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

Novembre 2011

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

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada sur la *Loi sur la protection des renseignements personnels* pour la période du 1er avril 2010 au 31 mars 2011, conformément à l'article 38 de la *Loi*.

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

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

(Original signé par)

Jennifer Stoddart

TABLE DES MATIÈRES

À PROPOS DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

La *Loi sur la protection des renseignements personnels*, qui est entrée en vigueur en 1983, oblige environ 250 ministères et organismes fédéraux à respecter le droit à la vie privée des personnes en limitant la collecte, l'utilisation et la communication de leurs renseignements personnels.

La *Loi sur la protection des renseignements personnels* permet également aux personnes de demander l'accès aux renseignements personnels les concernant qui pourraient être conservés par des organismes fédéraux. Si elles pensent que ces renseignements sont inexacts ou incomplets, elles ont aussi le droit, en vertu de la *Loi*, de demander une correction.

Message de la commissaire

Au cours de la décennie suivant les événements du 11 septembre, assurer la sûreté aérienne s'est effectué à un prix toujours plus élevé pour la vie privée. Un rituel moderne fastidieux nous oblige à enlever nos bottes ou nos souliers et à ouvrir nos bagages pour montrer des petits articles de toilette dans des sacs en plastique transparents. Nous avons le « choix » de subir une fouille par palpation effectuée par un étranger en uniforme ou de se placer en position de fouille dans un scanner entouré de verre. Nous acceptons que les transporteurs aériens et les gouvernements s'échangent nos programmes de voyage, nos numéros de passeport et d'autres renseignements personnels.

Nous faisons preuve de stoïcisme face à ce lourd processus, car il n'existe pas d'autre solution pour quiconque veut utiliser les aéroports canadiens. En contrepartie, nous nous attendons à un gain considérable : voyager en avion à l'abri des terroristes et des autres menaces.

Toutefois, en tant que commissaire à la protection de la vie privée, je considère que la question a une portée beaucoup plus vaste. En plus de devoir protéger la sécurité physique, l'État est tenu de respecter les personnes, c'est-à-dire de protéger leur dignité et leurs renseignements personnels.

Il ne s'agit pas d'un luxe, mais bien de l'une des assises de la relation de confiance entre les citoyens et leur gouvernement.

Le présent rapport annuel examine attentivement les pratiques de gestion des renseignements personnels du gouvernement fédéral — dans le contexte de la sûreté aérienne, de l'application de la loi et du fonctionnement quotidien du gouvernement.

Malgré de nombreux aspects positifs, le bilan n'est pas sans tache.

Par exemple, au cours d'une vérification des mesures de sécurité prises dans les aéroports, nous avons examiné les salles privées où les agents regardent les images générées par les scanners corporels et nous y avons trouvé une caméra de télévision en circuit fermé et un téléphone cellulaire. Nous n'avons trouvé que peu d'appareils capables d'enregistrer des

données, mais force est de constater qu'il y en avait, ce qui contrevient à ce que stipulent les règlements.

Nous avons aussi trouvé des documents de nature très délicate sur des incidents relatifs à la sûreté, rangés dans des bibliothèques ouvertes et des boîtes à des endroits où des passagers pouvaient se trouver.

DES RENSEIGNEMENTS EN QUANTITÉ TROP ÉLEVÉE

La collecte, par les autorités en matière de sécurité, de renseignements personnels au-delà de leur mandat nous préoccupe encore davantage — des renseignements sur des incidents qui ne posent aucune menace pour la sécurité aérienne ou qui, dans certains cas, ne constituent même pas une infraction.

Une autre vérification portant sur le contrôle qu'exerce la GRC sur ses bases de données opérationnelles soulève des inquiétudes quant à la gestion des renseignements personnels.

Par exemple, quand une personne est réhabilitée ou condamnée injustement, la GRC est supposée bloquer l'accès à tous les renseignements portant sur cet incident dans sa base de données, ce qui n'a pas été fait. Par conséquent, même si les gens ont le droit de voir leur vie reprendre un cours normal, des renseignements sur leurs antécédents peuvent toujours être échangés.

Il ne fait aucun doute que l'État a besoin de renseignements personnels pour fonctionner. Aucun gouvernement ne pourrait éviter une attaque terroriste, combattre le crime, émettre un passeport ou gérer un système d'imposition sans posséder de données sur les personnes.

La technologie de l'information moderne facilite ce processus. Les données peuvent être recueillies en plus grande quantité et plus rapidement que jamais. Elles peuvent aussi être traitées, manipulées, modifiées, conservées et communiquées plus facilement qu'avant.

Toutes ces données sont gérées dans le but d'améliorer l'exécution des programmes, la sécurité publique, l'efficacité de la gouvernance et la responsabilité.

Toutefois, comme le présent rapport l'indique, la présence d'une si grande quantité de renseignements personnels entre les mains du gouvernement peut aussi poser des risques pour la vie privée des personnes.

RISQUES POUR LA VIE PRIVÉE

Voici quelques exemples. Même le fait qu'une personne voyage au Canada avec une grosse somme d'argent ne regarde pas l'État, les autorités recueillent et s'échangent entre elles ce type d'information. Un voyageur fortuné devient ainsi un voyageur suspect.

Lorsqu'une condamnation est annulée, le casier judiciaire doit être scellé. Les renseignements ayant mené à une condamnation injuste continuent néanmoins de circuler et peuvent ruiner des carrières, voire des vies.

Un virulent opposant du gouvernement se rend compte que des renseignements médicaux de nature délicate le concernant se trouvent dans un cahier d'information ministériel et sont échangés entre de nombreux fonctionnaires qui n'ont aucune raison de connaître ces détails.

Un surplus de renseignements peut aussi mener à des fuites de données. Une constatation troublante, qui est exposée dans le présent rapport, est celle selon laquelle les atteintes à la vie privée les plus faciles à éviter découlent souvent d'une simple erreur humaine — comme celle d'un membre du personnel infirmier en psychiatrie d'un établissement correctionnel fédéral qui a oublié le dossier d'un patient dans un autobus municipal.

Ce sont là certaines des raisons pour lesquelles la *Loi sur la protection des renseignements personnels* établit des règles concernant la collecte, l'utilisation, le stockage, la conservation, la protection et la communication des renseignements personnels. Le présent rapport porte sur l'état de la gestion des renseignements personnels sous le régime de la *Loi* en 2010-2011. Il décrit ce que le gouvernement fait correctement ou non et indique les améliorations pouvant être apportées et soulignées par le Commissariat.

Une quantité de renseignements personnels sans précédent est disponible aujourd'hui et l'avidité de l'État pour ces renseignements est sans borne. La technologie utilisée pour gérer les données est de plus en plus sophistiquée, mais aussi vulnérable.

Dans ce contexte particulièrement difficile, le gouvernement du Canada ne peut faire aucun compromis sur la qualité du traitement des renseignements personnels des Canadiennes et des Canadiens.

Et cela doit s'appliquer en toutes circonstances.

Le Commissariat continuera de s'assurer que le gouvernement respecte ses obligations, et qu'il demeure digne de la confiance de la population et à la hauteur de ses attentes.

La protection de la vie privée en chiffres — 2010-2011

DEMANDES DE RENSEIGNEMENTS

Reçues	
Liées à la *Loi sur la protection des renseignements personnels*	**1 944**
Liées à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)	4 789
Demandes n'étant pas exclusivement liées à l'une ou l'autre des lois	2 188
Total des demandes reçues	***8 921***

Réglées	
Liées à la *Loi sur la protection des renseignements personnels*	**1 859**
Liées à la LPRPDE	4 762
Demandes n'étant pas exclusivement liées à l'une ou l'autre des lois	2 183
Total des demandes réglées	***8 804***

PLAINTES LIÉES À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Reçues	
Accès	328
Délais	251
Protection des renseignements personnels	129
Total des plaintes reçues	***708***

Réglées	
Règlement rapide	
Accès	30
Délais	6
Protection des renseignements personnels	42
Total	**78**
Enquête	
Accès	182
Délais	251
Protection des renseignements personnels	59
Total	**492**
Total des plaintes réglées	***570***

EXAMENS DES ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Reçues	52
Présentant un risque élevé	19
Présentant un risque faible	68
Total des évaluations examinées	***87***

VÉRIFICATIONS

Vérifications de la protection des renseignements personnels dans le secteur public	2

ACTIVITÉ JURIDIQUE LIÉE À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Avis juridiques	16
Litiges — décisions émises	0
Litiges — causes réglées	2

POLITIQUES ET AFFAIRES PARLEMENTAIRES

Lois ou projets de loi examinés sous l'angle de leurs répercussions sur la vie privée	19
Politiques ou initiatives du secteur public examinées sous l'angle de leurs répercussions sur la vie privée	51
Documents d'orientation stratégique rédigés	16
Témoignages devant des comités parlementaires sur des enjeux touchant le secteur public	14
Autres rencontres avec des parlementaires ou leur personnel	34

AUTRES ACTIVITÉS DU COMMISSARIAT

Secteur public	
Visites de la part d'intervenants externes	32
Activités publiques	2
Secteurs public et privé combinés	
Discours et exposés	112
Communiqués et autres outils de communication	57
Expositions et autres activités de promotion hors site	20
Publications distribuées	34 007
Visites sur le site principal du CPVP	2,22 millions
Visites sur les blogues et autres sites du CPVP	1,01 million
Nouveaux abonnements au bulletin électronique	321
Total des abonnements au bulletin électronique	1 013

LOI SUR L'ACCÈS À L'INFORMATION

Demandes reçues	63
Demandes réglées	64

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Demandes reçues	105
Demandes réglées	106

CHAPITRE 1

Bilan de l'année
Principales réalisations en 2010-2011

Voici les faits saillants concernant le travail accompli au cours du dernier exercice financier pour renforcer et protéger le droit à la vie privée des Canadiennes et des Canadiens dans le cadre de leurs interactions avec le gouvernement du Canada.

Pour obtenir plus de détails sur ces activités, veuillez consulter la section du présent rapport dont le numéro est inscrit dans la colonne de droite.

Vérifications du respect de la protection des renseignements personnels	
Nous avons réalisé deux vérifications de la conformité avec la *Loi sur la protection des renseignements personnels* au cours de l'année.	
Une d'entre elles visait à savoir si l'Administration canadienne de la sûreté du transport aérien (ACSTA) et les milliers d'agents qu'elle embauche à contrat dans les aéroports respectaient la vie privée des voyageurs et géraient bien les renseignements personnels en leur possession. Cette vérification a permis de constater que certains éléments d'un cadre de gestion de la vie privée sont en place, mais qu'il reste des lacunes importantes dans la pratique. Le principal problème est que l'organisme recueille certains renseignements personnels qui vont au-delà de son mandat. Par exemple, les agents de l'ACSTA alertent parfois la police lorsqu'ils rencontrent un voyageur interne transportant une grosse somme d'argent. Il est tout à fait légal de transporter de l'argent au Canada et, de toute façon, la question n'est pas liée à la sûreté aérienne et ne fait donc pas partie du mandat de l'ACSTA.	2.1

Nous avons également relevé des problèmes concernant la conservation de documents sensibles. Ainsi, nous avons trouvé des rapports d'incident sur des étagères ouvertes, sur le plancher et même dans une salle où se rendent les passagers retenus pour un contrôle plus approfondi. En outre, la vérification a permis de découvrir un téléphone cellulaire et une caméra de télévision en circuit fermé dans les salles où les agents visionnent les images générées par des scanners corporels, bien que les appareils de ce type y soient strictement interdits. Ces problèmes ont été réglés rapidement aussitôt qu'ils ont été portés à l'attention des responsables de l'ACSTA.	**2.1**
L'autre vérification portait sur la gestion des bases de données opérationnelles de la GRC, qui comprennent des renseignements échangés avec de nombreux services de police et institutions fédérales. Une des bases les plus connues est le Centre d'information de la police canadienne (CIPC), qui contient plus de 10 millions de documents et est consulté par environ 80 000 agents de la paix de plus de 3 000 services de police, des détachements de la GRC et des organismes fédéraux et provinciaux. La GRC dispose de politiques et de procédures pour protéger ces renseignements sensibles, mais nous avons aussi repéré des lacunes inquiétantes. Par exemple, dans le Système d'incidents et de rapports de police (SIRP), une base de données, la GRC ne dispose d'aucun processus pour supprimer l'accès à des renseignements qui sont liés à une infraction ayant fait l'objet d'une réhabilitation ou — pire encore — qui ont entraîné une condamnation injustifiée. La GRC s'est engagée à régler tous nos sujets de préoccupation.	**2.2**
Nous avons aussi fait le suivi de trois vérifications menées en 2008 et 2009. Les ministères concernés nous ont avisés que 32 des 34 recommandations que nous avions faites à la suite de ces vérifications ont été appliquées intégralement ou en grande partie.	**4.4**
Une enquête de suivi portait essentiellement sur les fichiers inconsultables de la GRC comprenant des données personnelles qui ne sont pas assujetties aux clauses sur l'accès de la *Loi sur la protection des renseignements personnels*.	**2.5**

Nous étions heureux d'apprendre que la GRC avait suivi notre recommandation de dépouiller les données et de supprimer toutes celles qui ne devraient pas y être. En mars 2011, seulement 190 des 5 288 dossiers qui se trouvaient dans le fichier national inconsultable de la GRC sur la sécurité nationale en mars 2008 n'avaient pas été supprimés. En outre, plus de 58 000 dossiers de renseignements sur la criminalité ont été supprimés.	2.5

Demandes de renseignements, plaintes et atteintes à la protection des renseignements personnels	
Notre unité de demandes de renseignements a répondu à 1 859 appels et lettres directement liées à la *Loi sur la protection des renseignements personnels* en 2010-2011, une diminution de 30 % par rapport à l'année précédente. Nous avons reçu 2 183 demandes de renseignements où il était impossible de déterminer quelle loi sur la protection des renseignements personnels s'appliquait ou qui n'étaient liées à aucune des deux lois. Étant donné que le nombre de visiteurs sur le site Web du Commissariat continue d'augmenter — 2,2 millions de visiteurs en 2010-2011, une augmentation de 31 % depuis 2007-2008 — nous supposons que de plus en plus de personnes se rendent en ligne pour trouver des réponses à leurs questions sur la protection de la vie privée.	5.1.1
Cette année, nous avons continué d'axer nos efforts sur les stratégies de règlement rapide permettant de résoudre une plainte sans enquête officielle. En tout, 78 des 570 plaintes réglées l'année dernière ont été réglées de cette manière, c'est-à-dire 14 % de notre volume de cas, par rapport à 6 % l'année précédente. Cette stratégie a eu des répercussions positives sur la rapidité de notre service. En moyenne, les cas réglés rapidement ont été fermés après 3,6 mois l'année dernière, ce qui a fait passer les délais de traitement globaux à 7,2 mois comparativement à 12,9 mois en 2009-2010.	5.1.2
Dans la grande majorité des 492 plaintes ayant fait l'objet d'une enquête complète en 2010-2011, des personnes avaient de la difficulté à accéder aux renseignements les concernant que possédait le gouvernement (182) ou se plaignaient du temps pris par le gouvernement pour répondre aux demandes d'accès (251). Près de 80 % des plaintes liées aux délais qui ont demandé une enquête ont été portées contre le Service correctionnel du Canada (150), l'Agence du revenu du Canada (24) ou le ministère de la Défense nationale (23).	5.1.4

Nous avons rendu des conclusions officielles après 443 enquêtes; les autres ont été abandonnées (41) ou réglées en cours d'enquête (8). Dans 63 % des cas, nous nous sommes prononcés en faveur du plaignant, souvent parce que l'institution ne lui avait pas donné accès à ses renseignements personnels en temps opportun. En général, quand la plainte n'est pas fondée, c'est parce que l'institution a correctement appliqué une des exceptions lui permettant de ne pas diffuser certains renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*. Sur les 570 plaintes réglées, 101 portaient sur des préoccupations relatives à la collecte, à l'utilisation, à la communication, à la conservation ou au retrait des renseignements personnels. Les circonstances variaient des cas les plus graves aux plus banals.	**5.1.4**
Un cas digne de mention concernait Anciens Combattants Canada. Nous avons appris qu'une grande quantité de renseignements personnels sensibles du plaignant, dont des renseignements médicaux, s'étaient retrouvés dans un cahier d'information préparé à l'intention de l'ancien ministre des Anciens Combattants. À titre d'exemple, avant la participation du plaignant à une conférence de presse sur la colline du Parlement, le ministre a reçu de l'information sur les antécédents médicaux du plaignant, le plan de traitement recommandé et les avantages reçus en tant qu'ancien combattant. De plus, les renseignements personnels de ce dernier ont été diffusés à grande échelle parmi les fonctionnaires du Ministère, qui n'auraient normalement eu peu ou pas du tout besoin d'avoir accès aux antécédents médicaux de l'homme concerné pour accomplir leurs tâches. Nous avons considéré que la plainte était fondée. Étant donné que l'enquête a révélé de graves problèmes systémiques, nous avons décidé de lancer une vérification complète du Ministère en 2011-2012.	**3.1**
D'autres atteintes à la vie privée étaient beaucoup moins évidentes, mais certainement inquiétantes pour les personnes concernées. Dans plusieurs cas, les renseignements personnels des Canadiennes et Canadiens ont été traités de façon inadéquate par des fonctionnaires : ils ont été laissés dans des endroits publics, oubliés dans un autobus ou envoyés par le système de courrier interne d'une prison sans même être mis dans une enveloppe.	**4.1.1** **4.1.2** **4.1.4**

Nous avons aussi soulevé des questions relatives à la façon dont Postes Canada évalue la validité des demandes de congé payé spécial pour prendre soin d'un parent souffrant. Nous avons conclu que l'organisme demande plus de renseignements que nécessaire, y compris de l'information sur des tiers.	**2.4.1**
En plus des plaintes déposées par des particuliers, nous avons reçu 64 rapports de ministères et d'organismes décrivant les cas où ils ont communiqué les renseignements personnels de Canadiennes et de Canadiens de manière inappropriée. Une politique du Conseil du Trésor oblige les institutions à signaler de telles atteintes au Commissariat en temps opportun. Nous avons reçu plus de rapports que jamais au cours du dernier exercice. Encore une fois, nous avons constaté que les incidents sont causés par la nonchalance : des cahiers laissés dans des véhicules de transport en commun et des avions, des coquilles sur des étiquettes d'adresse et des documents télécopiés au mauvais bureau. Comme c'est le cas chaque année, nous avons constaté que le traitement des demandes déposées en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels peut mener à la communication non intentionnelle de renseignements personnels qui auraient dû être protégés.	**4.2**
Un incident insolite a été signalé par Ressources humaines et Développement des compétences Canada : un problème technique touchant le tout nouveau portail en ligne de Service Canada permettait aux utilisateurs de voir les renseignements financiers et d'autres renseignements personnels des visiteurs précédents sur le site. Une vérification interne a permis de conclure que seulement 75 des 85 000 personnes qui avaient utilisé le site à sa première journée d'activité ont été touchées par le problème technique. Les essais ont démontré que la défaillance provenait de la clé d'accès, une caractéristique de l'architecture sous-jacente qui a été désactivée. Le Ministère continue de collaborer avec Bell Canada, qui fournit le service de clé d'accès au gouvernement, pour trouver une solution technique permanente et fiable.	**4.2.6**
Le rapport de cette année porte aussi sur les communications faites en vertu de l'alinéa 8(2)*m*) de la *Loi sur la protection des renseignements personnels*, qui stipule que les ministères et organismes gouvernementaux peuvent communiquer des renseignements personnels si des raisons d'intérêt public le justifient nettement ou si l'individu concerné en tirerait un avantage certain.	**4.5**

Il y a eu en tout 80 communications de cette nature, la grande majorité provenant du ministère des Affaires étrangères, du Service correctionnel du Canada et de la GRC. Entre autres exemples typiques, mentionnons le fait d'avertir une communauté avant la libération d'un détenu, d'informer les responsables provinciaux de la santé lorsque des voyageurs aériens ont peut-être été exposés à un voyageur atteint de la tuberculose ou de transmettre des avertissements concernant des professionnels qui ont des problèmes de nature disciplinaire ou autre.	4.5

Examens des évaluations des facteurs relatifs à la vie privée	
Nous avons examiné 87 évaluations des facteurs relatifs à la vie privée en 2010-2011, dont 19 de façon plus approfondie en raison de l'importance des risques pour la vie privée ou des vastes questions relatives à la société et aux droits de la personne qui sont en jeu. Les ministères et organismes doivent présenter de telles évaluations au Commissariat pour montrer qu'ils ont tenu compte des répercussions des programmes et activités proposés sur la vie privée et ont prévu des moyens pour atténuer les intrusions.	2.3
Un de nos examens portait sur un plan de l'ACSTA qui consistait à observer les passagers dans les zones de préembarquement des aéroports pour détecter les comportements suspects. Nous avons soulevé plusieurs préoccupations, dont la possibilité qu'un profil de risque soit établi de façon inappropriée en fonction de caractéristiques comme la race, l'origine ethnique, l'âge ou le sexe.	2.3.2
Une autre évaluation des facteurs relatifs à la vie privée examinée a été présentée par Citoyenneté et Immigration Canada et concernait l'utilisation de la biométrie pour identifier tous les non-Canadiens entrant au pays. Nous avons formulé un certain nombre de recommandations pour améliorer la protection des données et veiller à ce que celles-ci ne soient échangées avec d'autres pays que dans des circonstances rigoureusement contrôlées.	2.3.3
Nous avons aussi continué d'examiner une série d'évaluations des facteurs relatifs à la vie privée liées à un vaste projet en développement permettant à la GRC et aux forces policières provinciales, territoriales, autochtones et municipales d'échanger les données d'enquête qu'elles recueillent entre elles et avec des ministères fédéraux.	4.3

La structure d'échange de données s'appelle le Système national intégré d'information interorganismes (N-III). Les renseignements que l'on peut obtenir à partir de cette structure peuvent être subjectifs ou ne révéler aucun écart de conduite. Nous avons fait remarquer que, s'ils étaient utilisés dans un contexte inapproprié et sans les mesures de sécurité nécessaires, les renseignements pourraient porter préjudice à des personnes innocentes. Nous avons recommandé d'instaurer des mesures de sécurité et de contrôle pour régir l'échange de ces renseignements et favoriser la transparence et la responsabilité.	**4.3**

Politiques et affaires parlementaires	
Au cours du dernier exercice financier, nous avons comparu à 15 reprises devant des comités parlementaires pour aborder des questions liées au secteur public (à une exception près). Nous avons donné notre point de vue sur la transparence gouvernementale, l'exploitation sexuelle des enfants et le questionnaire long du recensement. Nous avons donné un aperçu des priorités du Commissariat au moment où le mandat de la commissaire a été prolongé pour une durée de trois ans. La sûreté aérienne est une source de préoccupation constante en raison des mesures législatives comme le programme Information préalable sur les voyageurs/Dossier du passager, le Programme de protection des passagers et le Secure Flight Program des États-Unis. Ces mesures ont entraîné la création de gigantesques bases de données gouvernementales, l'utilisation de listes secrètes de personnes interdites de vol, la surveillance étroite des voyageurs et des travailleurs dans les aéroports et l'échange de renseignements plus intensif avec des gouvernements étrangers. Dans le cadre de notre comparution devant un comité parlementaire à propos de la sécurité aérienne, nous avons souligné l'importance de la transparence, de la minimalisation de la collecte de données, de l'établissement de périodes de conservation limitées et de la création de mécanismes de recours solides et accessibles.	**3.5** **5.2**
La loi sur l'accès légal, par laquelle le gouvernement souhaite renforcer la capacité qu'ont les organismes de police et les agences de sécurité de consulter les données liées aux communications électroniques des citoyens, est une autre préoccupation.	**2.6.2**

La commissaire Stoddart et ses homologues provinciaux et territoriaux ont envoyé une lettre conjointe au sous-ministre de Sécurité publique Canada pour attirer l'attention sur les risques pour la protection de la vie privée qui pourraient découler de l'intention du gouvernement de modifier le régime légal gouvernant l'utilisation de la recherche, de la saisie et de la surveillance électroniques.	**2.6.2**

Soutenir les fonctionnaires	
Les Canadiennes et Canadiens comptent sur le gouvernement pour traiter leurs renseignements personnels avec tout le soin et le professionnalisme possibles. Toutefois, le gouvernement n'est pas une entité homogène; il s'agit de dizaines de milliers de personnes qui font généralement de leur mieux pour répondre aux exigences de la *Loi sur la protection des renseignements personnels*. Conscients du défi que doivent relever les fonctionnaires qui font face à l'énorme pression associée à la collecte et à la manipulation des données, nous avons tenté en 2010-2011 de fournir une aide technique au moyen d'ateliers, de séminaires et d'autres activités de sensibilisation. Par exemple, en mars, nous avons présidé le premier Forum sur les pratiques relatives à la protection de la vie privée, qui se voulait un lieu d'échange pour les fonctionnaires souhaitant apprendre et partager leur savoir lié à l'avancement de la protection de la vie privée dans le contexte de leur ministère.	**5.3**
Nous avons également consacré beaucoup d'efforts pour aider les institutions à s'adapter à la nouvelle directive gouvernementale sur les évaluations des facteurs relatifs à la protection de la vie privée. Nous avons organisé un deuxième atelier annuel pour aider plus de 100 participants à préparer de bonnes évaluations des facteurs relatifs à la vie privée. Durant l'atelier, nous avons lancé un document d'orientation détaillé sur nos attentes concernant ces évaluations. Ce document, intitulé *Nos attentes : Un guide pour la présentation d'évaluations des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada*, a été distribué dans l'ensemble de la fonction publique et est disponible sur notre site Web.	**5.3.1**

Le Commissariat a aussi demandé l'avis d'une vaste gamme d'experts dans les domaines de la protection de la vie privée et de la sécurité pour élaborer un document de référence visant à aider les décideurs, les praticiens et les citoyens à intégrer les mécanismes de protection de la vie privée aux nouveaux objectifs de sécurité publique et nationale.

Ce document, intitulé *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*, fournit des renseignements contextuels importants ainsi qu'une marche à suivre pour atteindre l'équilibre approprié.

2.6.1

L'utilisation accrue des renseignements biométriques comme les empreintes digitales et les images faciales est un autre domaine dans lequel nous avons offert des conseils.

La biométrie peut donner lieu à des systèmes d'identification performants et fiables, mais elle peut également poser des problèmes importants en ce qui concerne la protection de la vie privée, y compris la collecte secrète de données biométriques, la correspondance de données et la communication indésirable de renseignements secondaires compris dans les renseignements biométriques d'une personne.

Pour aider les institutions à peser le pour et le contre, le Commissariat a préparé un document d'introduction détaillé intitulé *Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée*. Ce document présente une méthode permettant de déterminer si diverses applications de la biométrie sont convenables et des recommandations pour élaborer des projets qui tiennent davantage compte de la vie privée.

2.7

Développement du savoir

La *Loi sur la protection des renseignements personnels* ne nous confie pas explicitement le mandat de sensibiliser le public, mais cela ne nous empêche pas d'entrer en contact avec ceux que nous servons pour les aider à mieux comprendre leur droit à la vie privée et la manière de protéger leurs renseignements personnels.

Ainsi, au cours de la dernière année, nous avons participé à 20 expositions et à d'autres activités promotionnelles hors site, distribué 34 000 publications, donné 112 discours et accueilli la visite de 32 intervenants. Nos sites Web et le blogue du Commissariat sont toujours des moyens prisés de diffuser de l'information puisque 3,23 millions de visites ont été enregistrées au cours du dernier exercice financier.

La protection de la vie privée en chiffres

5.5.1

Nous nous employons également à développer le savoir sur la protection de la vie privée et sur les nouvelles menaces pour les renseignements personnels.

À cette fin, nous avons commandé des recherches sur divers sujets, par exemple : les principales préoccupations des fonctionnaires qui travaillent dans les services d'accès à l'information et de protection des renseignements personnels des institutions fédérales; les lois et les pratiques des pays en voie de développement dans le domaine de la protection de la vie privée et de la collecte de données; les répercussions sur la vie privée des nouvelles technologies d'authentification intégrées aux systèmes de paiement en ligne.

CHAPITRE 2

Pour une réduction de la quantité de données

L'État pourrait-il se montrer moins avide de renseignements sur les citoyens?

Lorsque l'alpiniste britannique George Mallory s'est fait demander en 1924 pourquoi il souhaitait escalader le mont Everest, il aurait eu ce mot d'esprit devenu célèbre : « Parce qu'il est là. »

De nombreuses organisations du monde entier semblent animées par la même logique puisqu'elles s'empressent de constituer de véritables montagnes de renseignements personnels. Si l'information donne du pouvoir, pourquoi ne pas y aller à fond? Avoir des données, c'est bien. En avoir beaucoup, c'est encore mieux.

Le gouvernement du Canada, qui est déjà le plus grand dépositaire de renseignements personnels au pays, succombe lui aussi à cette tentation. Les données personnelles sont l'oxygène dont l'État a besoin pour gouverner. Sans elles, il n'y aurait ni revenus ni versements; il n'y aurait pas non plus de paix, d'ordre ou de bon gouvernement.

Malgré tout, il y a des limites. Les articles 4 à 6 de la *Loi sur la protection des renseignements personnels* précisent dans quelles conditions les ministères et organismes fédéraux peuvent recueillir, conserver et éliminer des renseignements personnels.

De manière générale, le gouvernement ne peut recueillir que les renseignements personnels ayant un lien direct avec ses programmes ou ses activités. Si cela est possible, les données doivent être recueillies auprès de la personne concernée. À quelques exceptions près, celle-ci doit être informée des fins de la collecte.

Lorsque les renseignements ont servi aux fins auxquelles ils ont été recueillis, ils peuvent être conservés pour une durée limitée et doivent être éliminés en conformité avec certaines règles.

Réduire la collecte au minimum

Il est sans nul doute beaucoup plus facile, à l'ère numérique, de tout recueillir plutôt que de dépouiller, trier et rejeter les renseignements personnels qui ne sont plus nécessaires.

Toutefois, la facilité et les raisons pratiques ne justifient pas la collecte et la conservation excessives de renseignements personnels. En effet, les limites imposées par la *Loi sur la protection des renseignements personnels* ont un fondement pratique et philosophique.

La limitation de la quantité de données personnelles entre les mains du gouvernement diminue les risques de communications accidentelles, d'erreurs ou d'omissions entraînant des décisions aberrantes qui ont souvent des conséquences graves pour les personnes touchées.

En outre, les gens ont le droit de vivre en paix et de façon anonyme, à l'abri des regards de l'État. Ce principe est le fondement du sentiment de confiance qui doit exister entre les citoyens et leur gouvernement. Il s'agit d'une manifestation du contrat social qui caractérise une nation éclairée.

Le présent chapitre examine en profondeur ce que nous avons appris en 2010-2011 sur les pratiques de gestion des renseignements personnels du gouvernement, dont la collecte, la conservation, le stockage sécuritaire et le retrait. Il comprend les sections suivantes :

2.1 Vérification de l'Administration canadienne de la sûreté du transport aérien

Chaque année, des dizaines de millions de voyageurs utilisent les aéroports canadiens. Pour avoir le droit de monter à bord de l'avion, ils doivent subir un contrôle de sécurité et accepter que leurs bagages soient contrôlés.

Il est largement admis que les contrôles contribuent à garantir la sécurité des passagers, ce que le Commissariat ne conteste pas. Nous croyons cependant que la sécurité et la protection de la vie privée ne sont pas des valeurs contradictoires et que les gains d'un côté n'entraînent pas nécessairement une perte de l'autre.

Bien au contraire, nous sommes d'avis qu'un solide cadre de contrôle de la gestion des renseignements personnels des passagers atténuera les risques pour la vie privée tout en favorisant la sûreté aérienne.

C'est dans ce contexte que nous avons examiné si l'ACSTA, l'organisme fédéral chargé de contrôler les passagers et les bagages, se conforme aux exigences de la *Loi sur la protection des renseignements personnels* relatives au traitement de l'information.

L'Autorité canadienne de la sécurité du transport aérien

L'ACSTA est une société d'État fondée en avril 2002 à la suite des attaques terroristes du 11 septembre 2001 aux États-Unis. Son mandat est de contrôler les passagers, l'équipage de bord, les bagagistes et le personnel d'entretien pour trouver les articles interdits.

L'ACSTA indique qu'au 31 mars 2010, elle comptait 530 employés et 6 790 agents de contrôle engagés à forfait. Au cours d'une année moyenne, elle contrôle 48 millions de passagers et 62 millions de sacs de voyage dans 89 aéroports canadiens.[1]

CONSTATATIONS

2.1.1 SCANNERS CORPORELS

Les scanners corporels que l'on retrouve dans bon nombre d'aéroports canadiens détectent les explosifs et les armes dissimulés sous les vêtements du voyageur.

[1] Administration canadienne de la sûreté du transport aérien. *Aller de l'avant : Rapport annuel de 2010*, http://www.catsa-acsta.gc.ca/File/Library/87/French/RapportAnnuel2010.pdf.

Pour protéger la vie privée des passagers, l'ACSTA a établi un cadre solide comprenant des mécanismes de contrôle qui empêchent de lier une image à un nom ou à tout autre renseignement personnel du passager. Les images sont envoyées électroniquement dans une salle de visionnement isolée afin que l'agent de contrôle ne puisse voir ou identifier le passager. En outre, les images ne peuvent être conservées ou imprimées et sont supprimées définitivement après le contrôle.

Nous avons cependant constaté que les procédures destinées à protéger la vie privée ne sont pas toujours suivies. Par exemple, l'agent qui regarde les images doit veiller à ce que l'écran n'affiche aucune image avant que quelqu'un entre dans la salle ou en sorte, mais ce n'est pas toujours le cas.

Nous avons également vu un agent apporter un téléphone cellulaire dans la salle de visionnement, ce qui est strictement interdit puisque ces appareils ont souvent la capacité d'enregistrer des séquences vidéo.

De plus, nous avons repéré une caméra de télévision en circuit fermé dans le plafond d'une salle de visionnement d'un aéroport. Cette caméra a été désactivée quand nous avons attiré l'attention de l'ACSTA sur cette question.

En raison des préoccupations liées à la vie privée relativement à l'utilisation des scanners corporels, nous avons recommandé à l'ACSTA de s'assurer que les procédures visant à protéger la vie privée sont comprises et appliquées et de surveiller constamment si elles sont respectées. Nous lui avons aussi recommandé d'inspecter physiquement toutes les salles de visionnement et de désactiver toutes les caméras de télévision en circuit fermé s'il y a lieu.

2.1.2 COLLECTE DE RENSEIGNEMENTS PERSONNELS

Les règlements applicables à l'ACSTA et les décrets connexes exigent que l'organisme avise les autorités quand les activités de contrôle mènent à la détection d'une menace pour la sûreté aérienne. Par conséquent, elle collecte de façon tout à fait justifiée les renseignements personnels des voyageurs qui transportent une arme, des explosifs, un dispositif incendiaire ou tout autre article qui constitue une menace la sûreté aérienne afin de signaler l'incident aux autorités compétentes.

Activités possiblement illicites

Parfois, la recherche d'une menace pour la sûreté aérienne permet accidentellement de trouver des preuves d'une autre activité, comme une tentative apparente d'importer des stupéfiants ou d'exporter une importante somme d'argent. Le trafic de stupéfiants et d'argent est illégal, mais ne constitue pas une menace pour la sûreté aérienne.

Dans de telles circonstances, l'ACSTA détient le suspect et avertit le service de police approprié ou un autre organisme d'application de la loi.

Il a cependant été déterminé que, lorsque les autorités chargées d'appliquer la loi ont été prévenues, le rôle de l'ACSTA prend fin. Par conséquent, la production de rapports d'incident sur des activités illicites qui ne posent aucune menace directe pour la sûreté aérienne est inappropriée.

Nous avons donc recommandé que l'organisme recueille seulement les renseignements personnels concernant les incidents relatifs à la sûreté aérienne.

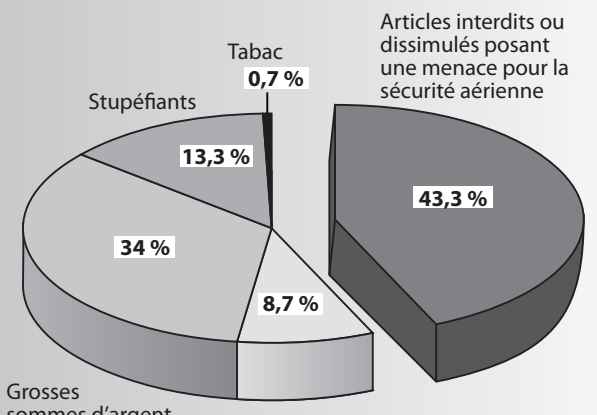
Transport d'argent à l'intérieur du pays

Nous avons aussi constaté que l'ACSTA recueille des renseignements personnels sur les voyageurs internes qui transportent de grosses sommes d'argent et transmet cette information à la police une fois que le passager a quitté la zone de fouille.

Ce n'est pas une infraction de transporter une importante somme d'argent lorsqu'on voyage au Canada. Étant donné que la personne est autorisée à franchir le point de contrôle, il est évident que l'argent découvert ne constitue pas une menace pour la sûreté aérienne et que la question ne fait pas partie du mandat de l'ACSTA.

Nous avons appris que l'ACSTA possède plus de 10 400 rapports d'incident dans ses dossiers. Nous avons prélevé un échantillon exploratoire de 150 rapports à examiner. Comme le montre le graphique, environ 57 % d'entre eux portaient sur des questions sans lien avec la sûreté aérienne.

VENTILATION DES RAPPORTS D'INCIDENTS PAR TYPE D'INCIDENT



À la lumière de notre analyse, nous avons conclu que l'ACSTA recueille des renseignements personnels au-delà de son mandat législatif. La petite taille de

notre échantillon ne permet cependant pas de connaître la proportion de rapports qui se trouvent dans les fonds de renseignements de l'ACSTA, mais qui ne devraient pas y être.

Nous avons recommandé que l'ACSTA adopte des mesures pour recueillir seulement les renseignements personnels directement liés à la sûreté aérienne.

2.1.3 SYSTÈME DE VÉRIFICATION ÉLECTRONIQUE DE L'AUTHENTICITÉ DES CARTES D'EMBARQUEMENT

Dans le contexte des contrôles préembarquement, l'ACSTA doit vérifier l'authenticité des cartes d'embarquement. Le Système de sûreté des cartes d'embarquement a été instauré en 2009 pour faciliter le processus. Il permet de saisir l'information imprimée sur la carte d'embarquement et d'autres données qui se trouvent dans un code à barres spécial.

Il est peut-être nécessaire d'afficher temporairement le contenu du code à barres de la carte d'embarquement pour que l'agent de contrôle puisse comparer l'information avec celle qui est imprimée sur la carte, mais nous avons remis en doute la nécessité de conserver des renseignements permettant d'identifier une personne dans la base de données du Système.

En effet, le Système a été créé pour détecter les cartes d'embarquement falsifiées, mais l'ACSTA utilise les données (plus précisément le nom des passagers) à d'autres fins, notamment pour répondre à des réclamations et à des plaintes de passagers et pour réagir à des atteintes et à des incidents relatifs à la sécurité (par exemple si une personne entre dans une zone réglementée sans avoir été contrôlée).

Règle générale, les renseignements personnels des passagers ne devraient pas être recueillis sous prétexte qu'ils pourraient servir éventuellement. L'ACSTA a démontré qu'elle doit recueillir des renseignements personnels enregistrés sur des cartes d'embarquement et des codes à barres pour remplir son mandat d'assurer la sûreté aérienne. Cependant, les passagers ne sont pas informés que les données sont conservées pendant 30 jours ou que cette information peut être communiquée aux homologues étrangers de l'ACSTA pour des raisons de sûreté aérienne.

Nous avons vivement encouragé l'ACSTA à faire connaître aux passagers les aspects suivants : les fins de la collecte, l'utilisation des données, les tiers auxquels l'information peut être communiquée et les circonstances dans lesquelles elle peut l'être et la période de conservation des données.

2.1.4 COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

Communication aux autorités

L'ACSTA est tenue de signaler les incidents relatifs à la sûreté aérienne à certaines autorités, dont le ministre des Transports, l'Agence des services frontaliers du Canada (ASFC) ou le transporteur aérien, le service de police ou l'exploitant d'aérodrome appropriés.

L'ACSTA n'est pas habilitée à chercher des articles de contrebande. Toutefois, elle communique avec les autorités lorsqu'elle découvre des stupéfiants illégaux ou d'importantes sommes d'argent durant le processus de contrôle. Elle fera connaître le nom du passager, les renseignements sur le vol et la description de l'article de contrebande présumé.

Nous nous sommes demandé si l'ACSTA avait le droit de communiquer avec la police ou l'ASFC à propos d'incidents sans lien avec la sûreté aérienne. Sous le régime de la *Loi sur la protection des renseignements personnels*, ce droit dépend de la compatibilité des communications avec le but dans lequel l'information a été obtenue.

Dans le contexte de son mandat, l'ACSTA obtient des renseignements personnels dans le but de contrôler les passagers et leurs bagages pour découvrir des articles interdits et des menaces pour la sûreté aérienne. Ce faisant, les agents tombent parfois sur d'autres articles illégaux comme des drogues illicites ou de l'argent de contrebande.

Pour déterminer si la communication de renseignements sur de telles découvertes à la police ou à d'autres autorités est un usage compatible au sens de la *Loi*, il faut se demander si on peut raisonnablement s'attendre à ce que l'ACSTA avertisse quelqu'un quand, dans le cadre de l'exécution de son mandat, ses agents découvrent par hasard des articles illicites qui ne font pas partie de ce mandat.

À notre avis, une personne pourrait raisonnablement s'attendre à ce que l'ACSTA avertisse les autorités compétentes quand des articles qui semblent illégaux sont accidentellement découverts. Les personnes consentent seulement à être fouillées, ou à ce que leurs bagages le soient dans le but d'éviter les menaces pour la sûreté aérienne, mais il serait déraisonnable de s'attendre à ce que l'on ferme les yeux sur un cas évident de possession d'objets illégaux.

Le fait d'avertir la police est directement lié au but premier dans lequel les renseignements ont été obtenus, c'est-à-dire pour protéger la sécurité publique et garantir le respect de la loi dans le contexte de la sûreté aérienne.

En revanche, aux termes de l'article 2.1.2, le fait de voyager au Canada avec de grosses sommes d'argent ne constitue pas une infraction. L'ACSTA n'a donc aucun motif d'alerter les autorités advenant la découverte d'argent comptant lors de ses contrôles de sécurité.

Pour que les pratiques de l'ACSTA soient conformes à la* Loi sur la protection des renseignements personnels*, nous recommandons à cette dernière d'arrêter de signaler à la police la découverte de grosses sommes d'argent dans les bagages d'une personne voyageant à l'intérieur des frontières canadiennes.

Communication aux transporteurs aériens

En plus d'informer la police des incidents qui ne sont pas liés à la sûreté aérienne, l'ACSTA fournit des renseignements personnels aux transporteurs aériens, ce qui n'est pas toujours approprié.

Par exemple, il convient d'informer un transporteur aérien qu'un passager est retardé au point de contrôle de sûreté, mais il n'est pas nécessaire de dévoiler les détails, comme le fait que des articles de contrebande ont été découverts dans les bagages de la personne.

Nous avons demandé à l'ACSTA de s'assurer que toutes les communications aux transporteurs aériens se limitent à ce qui est strictement nécessaire dans chaque cas.

2.1.5 PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES AÉROPORTS

L'ACSTA a confié la tâche de contrôler les passagers à onze entreprises privées. Chaque contrat comprend une entente de confidentialité qui établit les obligations des fournisseurs en matière de protection des renseignements personnels des passagers.

Pourtant, des visites des aéroports nous ont permis de découvrir des lacunes à cet égard : des rapports d'incident étaient rangés dans des bibliothèques ouvertes, sur le plancher et dans des meubles qui ne répondent pas aux exigences en matière de sécurité. Dans un aéroport, nous avons vu des rapports d'incident rangés dans des boîtes qui se trouvaient dans une salle de fouille privée.

L'entente de confidentialité exige que les fournisseurs de services de contrôle protègent les documents en conformité avec les procédures de l'ACSTA qui établissent les exigences concernant le stockage et la transmission de renseignements protégés et secrets.

Dans l'entente, l'ACSTA précise qu'elle déterminera quels renseignements se classent dans ces deux catégories. Cependant, elle ne l'avait pas fait au moment de notre vérification, ce qui pourrait avoir contribué à certaines des lacunes observées au chapitre du stockage.

Nous avons recommandé que l'ACSTA attribue une désignation de sécurité proportionnelle à la sensibilité des renseignements. Les agents de contrôle devraient prendre des mesures de sécurité matérielle qui répondent aux normes du Conseil du Trésor.

Nous avons aussi constaté que l'ACSTA ne surveille pas systématiquement le traitement des renseignements des passagers par les fournisseurs de services au moyen d'inspections ou de vérifications. L'organisme tenait pour acquis que les fournisseurs de services de contrôle traitaient les renseignements convenablement sans avoir l'assurance que c'était le cas.

Sans système de surveillance efficace, les fournisseurs de services peuvent se soustraire à leurs obligations de protection de la vie privée sans en subir les conséquences.

Nous avons recommandé que l'ACSTA veille à ce que les pratiques de gestion des renseignements personnels des passagers adoptées par les fournisseurs de services fassent l'objet d'inspections et de vérifications périodiques.

2.1.6 PRATIQUES DE CONSERVATION ET DE RETRAIT DES RENSEIGNEMENTS PERSONNELS DE L'ACSTA

Quand un incident relatif à la sûreté ou une atteinte à la sécurité surviennent, l'ACSTA recueille habituellement le nom du passager, les renseignements sur son vol, son adresse, son numéro de téléphone et un résumé de l'événement. Le rapport est télécopié au Centre des opérations de sûreté de l'ACSTA à Ottawa, puis versé dans le Système de collecte de données d'appels et d'incidents, le dépôt d'archivage électronique des rapports d'incident relatif à la sûreté.

La loi exige que les institutions fédérales élaborent des calendriers de conservation et de retrait de leurs documents. Ces calendriers indiquent combien de temps les documents seront conservés avant d'être détruits ou transmis à Bibliothèque et Archives Canada. Du point de vue de la protection des renseignements personnels, le calendrier de conservation et de retrait est important, car la conservation de documents pour une trop longue période peut causer préjudice à la personne concernée.

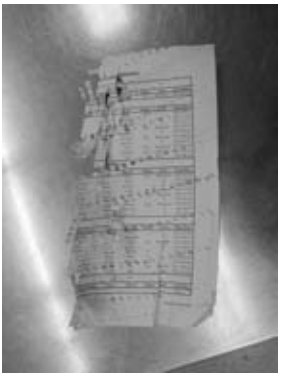
Nous avons constaté que l'ACSTA ne dispose d'aucun calendrier de conservation et de retrait des renseignements personnels dont elle a la garde. Par conséquent, l'administration centrale conserve indéfiniment les rapports d'incident relatif à la sûreté.

Nous avons recommandé que l'ACSTA supprime définitivement tous les documents qu'elle détient (en format électronique et sur papier) et qu'elle n'a pas le pouvoir de recueillir, notamment ceux qui sont liés à la découverte fortuite d'articles de contrebande, d'articles qui ont été considérés à tort comme des menaces pour la sûreté aérienne et d'importantes sommes d'argent transportées par des passagers.

L'ACSTA devrait établir un calendrier de conservation et de retrait des renseignements personnels recueillis dans le cadre de son mandat d'assurer la sûreté aérienne.

2.1.7 PRATIQUES DES FOURNISSEURS DE SERVICES EN MATIÈRE DE CONSERVATION ET DE RETRAIT DES RENSEIGNEMENTS PERSONNELS

Les contrats conclus entre l'ACSTA et les fournisseurs de services de contrôle n'établissent aucune exigence relative au retrait. Ce sont donc les fournisseurs de services de contrôle qui doivent élaborer et gérer le processus. Nous avons appris que les rapports d'incident sont généralement conservés pendant un an, puis détruits dans des déchiqueteurs sur place ou par des entreprises de déchiquetage privées.



Document encore lisible même après avoir été déchiqueté

Nous avons recueilli un échantillon de documents déchiquetés à l'un des aéroports où le déchiquetage est fait sur place.

Nous avons constaté que les documents n'étaient pas détruits en conformité avec la norme établie par le Conseil du Trésor. Il n'y a pas assez de données disponibles pour croire qu'il s'agit d'un problème systémique, mais cela démontre l'importance de surveiller les pratiques de retrait.

Nous avons cependant remarqué que l'ACSTA ne dispose d'aucun protocole de vérification lui permettant de surveiller la destruction de documents par des fournisseurs de services de déchiquetage hors site. Par conséquent, rien ne garantit que les personnes traitant les renseignements personnels des passagers font l'objet d'une enquête de sécurité du niveau approprié, que les rapports d'incident sont détruits de façon telle qu'ils ne peuvent être reconstruits et que les documents sont éliminés en temps opportun afin d'atténuer les risques de consultation non autorisée.

Nous avons recommandé à l'ACSTA de s'assurer que tous les contrats concernant le retrait des renseignements personnels soient conformes aux exigences du Conseil du Trésor et d'instaurer un protocole de surveillance des pratiques de retrait hors site.

2.1.8 AUTRES MESURES DE SÉCURITÉ EN PLACE

Notre vérification a révélé que d'autres mesures de sécurité importantes sont en place pour protéger les renseignements personnels.

- L'administration centrale de l'ACSTA est contrôlée par diverses mesures, y compris des agents de sécurité, des caméras de télévision en circuit fermé et un système d'alarme de détection d'intrusions. Des cartes de contrôle d'accès électroniques, des identificateurs biométriques et des armoires de sécurité limitent l'accès aux lieux et aux documents. Rien ne laisse croire que la sécurité des renseignements personnels pourrait être compromise par des mesures de sécurité matérielle inadéquates.

- L'ACSTA utilise un réseau privé qui relie l'administration centrale, les aéroports et les centres de données. Nous avons examiné l'architecture du réseau et trouvé des mesures adéquates pour protéger les renseignements personnels, dont des pare-feu, des technologies de détection et de prévention des intrusions, un système de gestion automatique des correctifs et des mécanismes pour contrôler l'accès. Les menaces et les risques ont été évalués et des essais de pénétration sont effectués chaque année pour cerner et corriger les faiblesses éventuelles.

- Les données extraites du code à barres de la carte d'embarquement sont transmises par un réseau sécurisé à un serveur local, puis à une base de données centrale. L'ACSTA a instauré des mécanismes de contrôle pour protéger les données pendant la transmission. De plus, les renseignements personnels enregistrés dans la base de données sont chiffrés.

- Les ententes de services avec les tiers comprennent des clauses satisfaisantes sur la protection de la vie privée. Par exemple, les renseignements personnels doivent être stockés au Canada; les mesures de sécurité et les mesures physiques doivent répondre aux normes du gouvernement fédéral sur la sécurité; les renseignements ne peuvent être utilisés à des fins secondaires; toute personne ayant accès à la base de données doit avoir une cote de sécurité du niveau secret.

- L'ACSTA a installé un système de télévision en circuit fermé pour observer et enregistrer les mouvements des passagers du moment où ils entrent dans la file d'attente pour subir le contrôle jusqu'à ce qu'ils aient été contrôlés par des agents. L'utilisation, la conservation et la communication des bandes vidéo, ainsi

que l'accès à celles-ci, sont soumis à des mécanismes de contrôle adéquats. En outre, l'ACSTA nous a informés qu'elle ne diffusera aucune bande vidéo sans y être obligée par un mandat ou une ordonnance d'un tribunal.

2.1.9 TRANSPARENCE

Les institutions fédérales sont tenues de décrire les renseignements personnels en leur possession dans *Info Source*, un répertoire publié par le Secrétariat du Conseil du Trésor. Nous avons cependant constaté que la version actuelle d'*Info Source* ne comprend aucune information sur la collecte de renseignements personnels par l'ACSTA.

Nous avons aussi constaté un manque de transparence relativement à l'utilisation de la télévision en circuit fermé dans les zones de contrôle des passagers. Seulement quatre des huit aéroports visités comprenaient des affiches que les passagers pouvaient voir, et elles disaient seulement que la zone *pouvait* être sous surveillance. On nous a confirmé que les caméras enregistrent continuellement les mouvements des passagers.

De plus, les passagers ne sont pas toujours informés des options qui s'offrent à eux lorsqu'ils subissent une fouille corporelle.

Les passagers choisis pour un contrôle supplémentaire ont le choix entre un balayage corporel, une fouille corporelle en public ou une fouille corporelle en privé, dans une salle ou une cabine fermée. Cependant, dans cinq aéroports, nous avons observé que les voyageurs se voient généralement offrir le choix entre le balayage corporel ou la fouille corporelle en public. La fouille corporelle en privé était rarement offerte.

***Nous avons recommandé à l'ACSTA de décrire toutes les catégories de renseignements personnels dont elle a la garde dans la prochaine version d'*Info Source.**

Dans un esprit de transparence, l'organisme devrait aussi veiller à ce que les passagers sachent qu'un système de télévision en circuit fermé est utilisé pour les surveiller et connaissent les trois options lorsqu'ils sont retenus pour une fouille corporelle supplémentaire.

2.2 Vérification de certaines bases de données opérationnelles de la GRC

2.2.1 APERÇU

Les responsables de l'application de la loi et de la justice pénale du Canada disposent d'un imposant réseau de systèmes de bases de données pour les aider à appliquer les lois, à prévenir les crimes, à mener des enquêtes et à maintenir la paix, l'ordre et la sécurité.

Aux fins de la vérification, nous avons examiné deux bases de données sélectionnées parmi l'ensemble de celles qu'utilise la Gendarmerie royale du Canada (GRC) dans le cadre de ses opérations de maintien de l'ordre et de prévention du crime. Les renseignements que contiennent ces deux bases de données sont communiqués à un large éventail de partenaires du secteur de la sécurité publique.

- Le ***Centre d'information de la police canadienne*** (CIPC) offre un service informatisé de stockage et de recherche d'informations sur les crimes et les criminels. Le CIPC contient plus de dix millions de documents qui concernent, par exemple, des permis de conduire et des plaques d'immatriculation, des véhicules et des bateaux volés, des mandats d'arrêt, des personnes et des biens disparus, des casiers judiciaires, des empreintes digitales, des armes à feu enregistrées et des enfants disparus.

  Il permet à plus de 80 000 agents de la paix de plus de 3 000 services de police, détachements de la GRC et organismes fédéraux et provinciaux de se connecter au système informatique central. Les tribunaux, les commissions des libérations conditionnelles et des ministères et organismes gouvernementaux comme le Service correctionnel du Canada, l'Agence des services frontaliers du Canada, l'Agence du revenu du Canada et Passeport Canada ont aussi recours au CIPC.

  À propos de la police montée

  La GRC compte environ 30 000 membres. Elle applique les lois fédérales partout au pays et fournit des services d'enquête et de soutien opérationnel à plus de 500 organismes canadiens d'application de la loi et de justice pénale. Elle offre aussi des services de police à forfait dans toutes les provinces, à l'exception du Québec et de l'Ontario, ainsi que dans les trois territoires et dans près de 200 municipalités.

  L'information contenue dans le CIPC est diffusée à l'échelle internationale par le biais d'INTERPOL et est communiquée aux organismes américains d'application de la loi comme United States Customs and Border Protection.

Même le Bureau d'assurance du Canada, l'association sectorielle nationale du marché de l'assurance de dommages, a accès au CIPC.

Plus de 200 millions de demandes ont été traitées à partir de 40 000 points d'accès en 2009.

- Le ***Système d'incidents et de rapports de police*** (SIRP) est le système de gestion des dossiers opérationnels de la GRC. Le SIRP a été instauré en 2003 et est utilisé par la GRC et 23 services de police partenaires qui, en général, comptent moins de 300 agents et ne possèdent pas leur propre système électronique de gestion des dossiers.

  Le SIRP contient des renseignements sur les gens qui ont été en contact avec la police en tant que suspects, victimes, témoins ou contrevenants, depuis le signalement de l'incident jusqu'à la conclusion définitive de l'affaire. Environ 1,6 million de dossiers d'incidents sont traités chaque année.

En vertu des pouvoirs conférés au Commissariat par la *Loi sur la protection des renseignements personnels*, nous avons vérifié la conformité de la GRC avec les exigences de la *Loi* relatives à la collecte, à la protection, à la conservation et au retrait des renseignements personnels stockés dans le CIPC et le SIRP.

Nous avons notamment examiné :

- les politiques et les procédures de la GRC régissant l'accès au CIPC et son utilisation;
- les politiques et les procédures relatives à la suppression des renseignements personnels du SIRP devenus superflus;
- les pratiques de la GRC concernant l'examen de la conformité aux modalités d'utilisation du CIPC et du SIRP;
- la gestion des droits d'accès au SIRP.

Utilisation des systèmes

Une agente de la GRC arrête un conducteur pour excès de vitesse. À l'aide de l'ordinateur qui se trouve dans sa voiture, elle entre une requête dans le CIPC pour voir si le véhicule a été volé ou si le conducteur est visé par un mandat non exécuté. Elle peut ensuite faire une recherche dans le SIRP pour savoir si le véhicule ou le conducteur ont été impliqués dans d'autres incidents. Un dossier d'incident est créé dans le SIRP pour prendre note de l'événement. Le dossier sera mis à jour au fil de l'évolution de l'affaire.

Nous n'avons pas examiné comment les renseignements personnels contenus dans ces bases de données sont utilisés, ni les mesures de protection des données prises par les

partenaires municipaux, provinciaux, territoriaux et internationaux qui ont accès aux données par le biais d'ententes officielles d'échange de renseignements.

2.2.2 IMPORTANCE DE CET ENJEU

Le CIPC et le SIRP contiennent tous deux une grande quantité de renseignements personnels sensibles qui, s'ils étaient utilisés ou communiqués de façon inappropriée, pourraient entraîner des répercussions considérables sur la réputation, l'employabilité et la sécurité des personnes touchées. Une atteinte à la sécurité peut aussi mettre en péril des enquêtes policières en cours.

Chaque année, la GRC produit un rapport sur les atteintes à la sécurité liées au CIPC. Certaines d'entre elles sont causées par la consultation non autorisée ou l'utilisation inappropriée de renseignements personnels appartenant à d'autres personnes.

La GRC a aussi constaté que certains services de police contrevenaient à la politique du CIPC en diffusant des détails sur des condamnations, des remises en liberté ou des réhabilitations à des employeurs sans le consentement éclairé des employés éventuels.

La GRC est responsable du stockage, de la récupération et de la communication des renseignements judiciaires partagés au nom des organismes agréés de justice pénale et des autres organismes partenaires. Elle est dans l'obligation de protéger la vie privée des personnes, et donc les renseignements personnels dont elle a la charge.

2.2.3 CONSTATATIONS

Centre d'information de la police canadienne (CIPC)

- **Politiques et procédures**

La GRC dispose de politiques et de procédures pour régir l'accès aux données du CIPC et l'utilisation de celles-ci de façon à protéger les renseignements personnels des Canadiennes et Canadiens. Entre autres, une stratégie d'atténuation des risques liés à la technologie de l'information oblige les organismes à adopter des protocoles d'identification et d'authentification robustes pour s'assurer que tous les utilisateurs soient légitimes.

Nous avons néanmoins découvert que les infrastructures du tiers des organismes étaient soumises à des contraintes qui empêchaient la mise en place de tels protocoles.

Nous avons également examiné le protocole d'entente (PE) dont se sert la GRC pour établir les conditions d'utilisation du CIPC par les organismes. Des PE ont été conclus

avec les organismes dont les pouvoirs d'application de la loi sont limités ou qui jouent des rôles complémentaires dans le cadre de l'application de la loi.

Par contre, au moment de notre vérification, des ententes devaient être signées avec environ 25 % des services de police qui avaient déjà obtenu l'accès dans le cadre de leur rôle général de maintien de l'ordre.

Nous avons recommandé que le Centre d'information de la police canadienne établisse des échéanciers précis relativement à la conclusion de PE renfermant des dispositions sur la protection de la vie privée, avec tous les services qui n'auraient pas encore signé une telle entente

- **Atteintes**

Notre vérification a montré que des atteintes à la protection des renseignements personnels ont eu lieu, mais relativement rarement. Des mécanismes sont en place pour enquêter sur ces atteintes et prendre des mesures à la suite des enquêtes.

Bon nombre de ces atteintes découlaient de requêtes effectuées dans le CIPC à des fins personnelles. La GRC a récemment découvert que certains services de police transmettaient des renseignements sur les casiers judiciaires tirés du CIPC à des employeurs. Des données liées aux condamnations, aux remises en liberté ou aux réhabilitations étaient diffusées sans le consentement éclairé de l'employé éventuel.

Des atteintes à la sécurité des données peuvent entraîner, selon leur gravité, l'émission d'une directive de la GRC, une modification de la politique du CIPC, une réprimande, une suspension ou un licenciement.

Système d'incidents et de rapports de police (SIRP)

- **Suppression des données**

La loi prévoit que tous les dossiers créés dans le SIRP doivent être supprimés à la fin de la période de rétention établie pour chaque catégorie de données. Si les dossiers ne sont pas supprimés, ils demeurent facilement accessibles.

Avant leur suppression, les dossiers sont évalués afin de déterminer s'ils devraient être archivés par Bibliothèque et Archives Canada. Nous avons constaté que la base de données du SIRP est conçue pour supprimer automatiquement les dossiers pour lesquels la date de retrait a été atteinte, à moins que ceux-ci ne possèdent une valeur archivistique.

Cela dit, même s'il existe une fonctionnalité qui permet de supprimer les données, nous avons constaté que la GRC l'a désactivée afin d'extraire des données statistiques.

***Une organisation qui conserve des renseignements personnels plus longtemps que ce qui est nécessaire contrevient à la* Loi sur la protection des renseignements personnels. *Nous avons donc recommandé que la GRC supprime les données qui doivent l'être afin de se conformer à la* Loi.**

La GRC a répondu qu'elle avait demandé à des employés de mettre au point une solution statistique et qu'une fois que celle-ci aurait été mise en œuvre, les données concernées seraient supprimées comme l'exige la loi.

Lors de notre examen des procédures de suppression prévues par la loi, nous avons également constaté que la GRC n'avait pas encore mis en place de processus visant à retirer l'accès aux dossiers liés à des infractions pour lesquelles il y a eu réhabilitation ou à des condamnations injustifiées. En cas de réhabilitation ou de condamnation injustifiée, les dossiers sont censés être retirés et ne devraient plus être accessibles au moyen du SIRP.

Il est important que les renseignements relatifs aux infractions commises par les délinquants canadiens réhabilités ne soient pas communiqués à tort puisque cela risquerait de nuire à leur capacité d'obtenir un emploi, de voyager, d'étudier et de faire du bénévolat au même titre que n'importe quel autre Canadien. La *Loi canadienne sur les droits de la personne* interdit la discrimination fondée sur l'état de personne graciée. Le droit de ne faire l'objet d'aucune discrimination est doublement important dans les cas où une personne a été condamnée à tort.

Afin d'atténuer le risque de communication illicite ou inappropriée, nous avons recommandé que la GRC mette en place des processus visant à retirer l'accès aux dossiers de la base de données du SIRP qui se rapportent aux infractions pour lesquelles il y a eu réhabilitation ou aux condamnations injustifiées.

- **Accès et suivi des activités**

La politique adoptée par la GRC prévoit que l'accès au SIRP soit révoqué lorsque l'utilisateur n'en a plus besoin pour accomplir les fonctions liées à son poste ou s'il n'a pas accédé au système pendant 14 mois.

La GRC a toutefois été incapable de démontrer qu'elle effectue un suivi systématique de l'utilisation du SIRP afin de s'assurer que les politiques qui en régissent l'utilisation sont respectées.

Nous avons en effet constaté qu'il n'existe aucune mesure de suivi actif des comptes des utilisateurs du SIRP et de l'utilisation que ces derniers font du système. Nous avons remarqué que plus de 1 000 utilisateurs autorisés n'avaient pas accédé au SIRP depuis 14 mois ou plus.

Nous avons aussi constaté que le SIRP permet le suivi des activités des utilisateurs au moyen d'un journal de vérification. Les renseignements consignés permettent de savoir exactement quels dossiers ont été visionnés et quelles modifications ont été apportées.

La GRC nous a cependant informés que, lorsqu'elle soupçonne un utilisateur d'utiliser le système à mauvais escient, les efforts requis pour consolider et examiner les entrées du journal de vérification nuisent à sa capacité de faire enquête. Le SIRP comprend un outil automatisé d'examen du journal de vérification, mais celui-ci n'a pas encore été activé. Il est donc très laborieux d'extraire les détails des activités d'un utilisateur et, par conséquent, de faire enquête sur les soupçons d'utilisation abusive.

Nous avons recommandé que la GRC examine régulièrement le statut des comptes des utilisateurs du SIRP et révoque l'accès au système lorsque les employés n'ont plus besoin de l'utiliser dans le cadre de leurs fonctions.

Afin de faciliter les enquêtes sur l'accès non autorisé aux renseignements personnels conservés dans le SIRP, nous recommandons en outre que la GRC active l'outil automatisé d'examen du journal de vérification.

- **Vérifications de la conformité**

Nous avons constaté que la GRC avait conclu des protocoles d'entente (PE) avec tous ses organismes partenaires afin de veiller à ce que les données conservées dans le SIRP ne soient utilisées qu'à des fins légitimes d'application de la loi.

Les PE, qui demeurent en vigueur pendant cinq ans, à moins d'une résiliation à juste titre, confèrent à la GRC le pouvoir d'effectuer un suivi de l'utilisation qui est faite de ses réseaux et par certains employés ainsi que de visiter périodiquement les locaux des services de police partenaires.

La GRC a toutefois été incapable de démontrer qu'elle exerce systématiquement le pouvoir qui lui est conféré afin de s'assurer que ses partenaires utilisent les renseignements personnels conservés dans le SIRP conformément aux conditions énoncées dans les protocoles d'entente conclus.

En effet, nous avons constaté que peu de vérifications avaient déjà été menées. Bien que tous les services de police partenaires de l'Alberta aient fait l'objet d'une vérification,

seuls quelques organismes de la Nouvelle-Écosse et aucun de l'Île-du-Prince-Édouard ont été soumis à une telle vérification.

Nous avons recommandé que la GRC adopte un processus d'examen qui soit uniforme et à intervalles réguliers afin de veiller à ce que tous les utilisateurs se conforment aux politiques et aux procédures régissant l'utilisation des renseignements personnels conservés dans le SIRP.

La GRC s'est engagée à donner suite à toutes les préoccupations soulevées dans notre vérification.

2.3 Évaluations des facteurs relatifs à la vie privée concernant la collecte de renseignements personnels

2.3.1 APERÇU

L'évaluation des facteurs relatifs à la vie privée est un outil important pour aider les institutions fédérales à examiner les répercussions sur la vie privée d'activités ou de programmes nouveaux ou ayant subi des modifications importantes.

L'une des raisons pour lesquelles les évaluations des facteurs relatifs à la vie privée sont si utiles est qu'elles incitent les institutions fédérales à tenir compte des répercussions sur la vie privée des initiatives proposées dès le début du processus d'élaboration.

Dans le meilleur des mondes, le processus d'évaluation des facteurs relatifs à la vie privée devrait aider les institutions fédérales à justifier les programmes et les activités susceptibles d'entraîner une atteinte à la vie privée à l'aide de quatre questions : Le projet est-il absolument nécessaire? Est-il susceptible d'atteindre efficacement les objectifs visés? L'atteinte prévue à la vie privée est-elle proportionnelle aux avantages obtenus? Y a-t-il des moyens moins envahissants de parvenir aux mêmes fins?

Une fois qu'elles ont répondu de façon satisfaisante aux quatre questions, les institutions fédérales doivent démontrer que les renseignements recueillis seront protégés. Nous encourageons donc les initiateurs d'un projet à examiner les dix principes relatifs à l'équité dans le traitement de l'information reconnus à l'échelle internationale pour la gestion des renseignements personnels. Ces principes prévoient, entre autres, la collecte des renseignements appropriés, la limitation de la collecte et la mise en œuvre de mécanismes de protection afin de réduire les risques d'atteintes à la sécurité des données.

Nouvelle directive

Le 1er avril 2010, la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (SCT) a remplacé la Politique d'évaluation des facteurs relatifs à la vie privée qui avait été adoptée en 2002. Même si le contenu de la Directive diffère quelque peu de celui de la Politique, les institutions fédérales sont toujours tenues de réaliser une évaluation des facteurs relatifs à la vie privée dès les premières étapes de l'élaboration d'initiatives qui comportent des risques liés à la vie privée, et de la présenter au Commissariat.

Nous lisons et évaluons tous les dossiers que nous recevons, et nous procédons à un examen plus approfondi lorsque nous estimons qu'un programme ou qu'une activité comporte des risques importants pour la protection de la vie privée ou soulève des questions en matière de protection de la vie privée qui sont liées aux droits de la personne ou à des enjeux de société plus vastes. Lorsque c'est le cas, nous communiquons aux ministères des recommandations détaillées et effectuons un suivi afin de nous assurer que les risques ont été atténués.

Nous n'approuvons aucune évaluation ni n'avalisons aucun projet ou proposition lors de notre examen. Les recommandations et les conseils que nous formulons au sujet des améliorations pouvant être apportées aux projets visent à mieux protéger la vie privée des Canadiennes et Canadiens. Même si les institutions ne sont pas tenues de prendre en compte nos conseils ou de mettre en œuvre nos recommandations, nous constatons que la plupart sont ouverts à nos commentaires et collaborent avec nous afin de résoudre ou d'atténuer les problèmes pour la vie privée.

Nous avons reçu 52 évaluations des facteurs relatifs à la vie privée au cours du dernier exercice, ce qui représente une diminution importante par rapport aux 102 évaluations que nous avons reçues au cours de l'exercice précédent. Nous ne connaissons pas les raisons de cette diminution. Il est possible que les institutions aient besoin de temps pour mettre en œuvre de nouvelles procédures en vertu de la nouvelle directive. Il est aussi possible que le grand nombre d'évaluations reçues en 2009-2010 soit attribuable au fait que les institutions ont voulu élaborer des évaluations des facteurs relatifs à la vie privée en vertu de l'ancienne politique.

Nous avons utilisé un processus de tri afin de concentrer nos ressources sur les dossiers prioritaires. Nous avons donc examiné 19 dossiers liés à des projets qui, à notre avis, représentaient le plus de risque pour la vie privée. Soixante-huit autres dossiers liés à des projets représentant un risque moins élevé ont également fait l'objet d'un examen.

Vous trouverez ci-dessous une description de plusieurs initiatives pour lesquelles nous avons examiné l'évaluation des facteurs relatifs à la vie privée au cours du dernier

exercice ainsi qu'un résumé des conseils fournis et les questions qui continuent de nous préoccuper.

Comme le processus d'examen se veut itératif et renouvelable, il nous arrive fréquemment de fournir des conseils au sujet de plusieurs versions de la même évaluation des facteurs relatifs à la vie privée, à mesure que les initiatives progressent de l'étape du lancement à celle de la mise en œuvre.

2.3.2 ADMINISTRATION CANADIENNE DE LA SÛRETÉ DU TRANSPORT AÉRIEN

Programme d'observation du comportement des passagers

Nous avons reçu une évaluation préliminaire des facteurs relatifs à la vie privée de l'Administration canadienne de la sûreté du transport aérien (ACSTA) pour le projet pilote d'observation du comportement des passagers.

Le Programme d'observation du comportement des passagers est une mesure de contrôle à l'aéroport fondée sur l'observation des passagers qui font la file au contrôle de sécurité pré-embarquement dans le but de repérer tout comportement suspect.

Les agents de l'ACSTA qui ont reçu une formation sur l'observation du comportement des passagers peuvent aborder des passagers, parler brièvement avec eux et demander à voir leurs documents d'identité et de voyage. Selon la façon dont la conversation s'est déroulée, les agents peuvent alors aiguiller les passagers vers un deuxième contrôle de sécurité.

À la suite de chaque interaction avec un passager, les agents remplissent une fiche dans laquelle ils décrivent l'incident ainsi que l'apparence du passager. Cette fiche ne contient aucun renseignement permettant d'identifier le passager, comme son nom ou son adresse.

Nos préoccupations

Lors de notre examen de l'évaluation des facteurs relatifs à la vie privée soumise par l'ACSTA, nous nous sommes posé des questions au sujet de l'efficacité de cette initiative pour ce qui est de repérer des menaces pour la sûreté aérienne. Nous avons mis en doute la nécessité de ce programme compte tenu du grand nombre de procédures et de programmes de sécurité déjà en place.

Nous avons notamment noté des risques de profilage inapproprié axé sur le risque et fondé sur des caractéristiques comme la race, l'origine ethnique, l'âge ou le sexe.

Nous avons également fait remarquer que l'ACSTA semble se diriger vers un contrôle fondé sur l'identité, ce qui représente un changement important dans ses opérations, auparavant fondées sur le contrôle des objets représentant un risque pour la sûreté aérienne.

Le fait que les efforts déployés dans le cadre du projet pilote d'observation du comportement des passagers aient été autorisés par une ordonnance provisoire rendue en vertu de la *Loi sur l'aéronautique* au lieu d'être prescrits par règlement nous a en outre inquiété. En vertu de la *Loi*, le ministre des Transports peut rendre des ordonnances provisoires si des mesures immédiates sont requises afin de lutter contre une menace grave ou un risque important pour la sûreté aérienne. Ces ordonnances sont rendues sans qu'un débat n'ait lieu au Parlement et sans que le public ait l'occasion de formuler des commentaires. Or, nous ne croyons pas que ce soit justifié pour un programme continu comme celui-ci.

Notre recommandation

Nous avons recommandé que des initiatives comme celles du programme d'observation du comportement des passagers soient autorisées par voie de règlement plutôt qu'au moyen d'une ordonnance provisoire. Les règlements sont publiés dans la* Gazette du Canada *afin que le public puisse les examiner et formuler des commentaires. Nous croyons que cette approche favoriserait un processus plus ouvert et transparent ainsi qu'un meilleur examen d'une mesure comportant des risques possibles pour la vie privée.

Pour l'instant, l'ACSTA a mis en place des affiches informant les passagers qu'ils pourraient avoir à présenter une pièce d'identité au poste de contrôle et nous a assurés que les interactions avec les passagers dans la file d'attente étaient effectuées le plus discrètement possible. L'ACSTA a également invité les employés du Commissariat à observer le projet pilote à l'aéroport international de Vancouver en juin 2011 afin de mieux évaluer le Programme.

2.3.3 CITOYENNETÉ ET IMMIGRATION CANADA

Protocole sur l'échange de données de grande valeur de la Conférence des cinq nations et Projet de biométrie pour les résidents temporaires

Le gouvernement du Canada s'apprête à utiliser la biométrie pour identifier tous les non-Canadiens qui entrent au Canada. Les mesures mises en œuvre s'adresseront, dans un premier temps, aux personnes qui doivent obtenir un visa à titre de visiteurs, d'étudiants ou de travailleurs temporaires, ainsi qu'aux demandeurs d'asile et aux personnes visées par une mesure d'exécution de la loi sur l'immigration.

Citoyenneté et Immigration Canada nous a demandé conseil en ce qui a trait à deux initiatives de contrôle de l'immigration fondées sur la collecte et l'utilisation d'identifiants biométriques, comme les empreintes digitales et les photographies numériques. Le Ministère, l'Agence des services frontaliers du Canada et la GRC participent à ces initiatives.

- En vertu du Protocole sur l'échange de données de grande valeur de la Conférence des cinq nations, les données biométriques requises aux fins du contrôle de l'immigration sont mises en commun par le Canada, l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.

- En vertu du Projet de biométrie pour les résidents temporaires, qui doit faire l'objet d'une mise en œuvre graduelle en 2013, les visiteurs, les travailleurs étrangers temporaires et les étudiants qui présentent une demande de visa devront s'inscrire à l'étranger et fournir les empreintes des dix doigts et une photographie numérique. Ces données seront comparées aux données fournies lors de l'inscription lorsque la personne se présentera à un point d'entrée au Canada.

Nos recommandations

En ce qui concerne les deux initiatives, nous avons demandé à Citoyenneté et Immigration de veiller :

- ***à ce que l'utilisation de la biométrie soit à la fois nécessaire et efficace afin de repérer et de prévenir les cas de fraude;***
- ***à ce que la communication de renseignements de nature délicate, en particulier dans le cas des personnes vulnérables comme les demandeurs d'asile, soit effectuée avec prudence et encadrée par des mesures de protection et des protocoles stricts;***
- ***à ce qu'une attention spéciale soit accordée à la protection des empreintes digitales, des photographies et des documents d'identification primaires recueillis par les centres d'inscription privés à l'étranger;***
- ***à ce que les critères pour la communication des données biométriques à d'autres pays soient établis avec prudence et à ce que la communication des données soit limitée aux cas les plus graves seulement.***

2.3.4 COMMISSION DE LA FONCTION PUBLIQUE

Stratégie de surveillance de l'impartialité politique

Nous avons abordé, dans notre rapport annuel de l'année dernière, nos préoccupations à l'égard de l'évaluation des facteurs relatifs à la vie privée élaborée pour un programme de la Commission de la fonction publique visant à recouper des bases de données gouvernementales de fonctionnaires anciens ou actuellement en poste avec des listes de candidats aux élections fédérales, provinciales et municipales.

Selon l'information qui nous a été fournie, la Stratégie de surveillance de l'impartialité politique visait également la surveillance d'Internet, y compris des sites des médias, des sites Web personnels et des sites de réseautage social comme Facebook, afin de repérer toute activité politique potentiellement inappropriée menée par des fonctionnaires.

Depuis la publication de notre rapport, la Commission nous a indiqué que l'élaboration de l'initiative n'avait jamais été achevée, qu'elle n'avait pas été mise en œuvre et avait été abandonnée.

2.4 Enquêtes sur des plaintes concernant la collecte de renseignements personnels

2.4.1 POSTES CANADA EXIGE TROP DE RENSEIGNEMENTS POUR LES DEMANDES DE CONGÉ

Une employée de Postes Canada a présenté une plainte concernant la grande quantité de renseignements personnels recueillis par son employeur lorsqu'elle a présenté deux demandes de congé payé spécial afin de prendre soin d'un membre de sa famille qui était malade.

Le formulaire de demande utilisé vise en fait seulement à aider les superviseurs à décider s'il y a lieu ou non d'accorder un congé. Le nombre de questions est laissé à la discrétion du superviseur. Toutefois, dans ce cas, le superviseur de la plaignante lui a remis à tort le formulaire intégral et lui a demandé de le remplir elle-même.

Le formulaire exigeait un grand nombre de renseignements personnels au sujet de la demanderesse, de la personne malade et même de tierces parties. Par exemple, on voulait savoir si un autre employé de Postes Canada avait présenté une demande de congé afin de prendre soin de la même personne.

Pendant l'enquête sur la plainte, Postes Canada nous a indiqué qu'elle recevait environ 3 000 demandes de congé spécial chaque année, ce qui fait au total plus de 125 000 heures de travail.

Au fil des années, les règlements d'arbitrage rendus en vertu de la convention collective ont permis de façonner la façon dont cette catégorie de congé est administrée. Ces règlements obligent Postes Canada à recueillir de grandes quantités d'information afin de s'assurer que les demandes de congé sont étudiées d'une façon juste et raisonnable.

Postes Canada se soucie par ailleurs de la prévention de la fraude et de l'utilisation abusive de ce congé pour une durée indéterminée. Nous reconnaissons l'obligation de l'organisation à cet égard, mais nous estimons tout de même qu'une trop grande quantité de renseignements personnels sont recueillis. Nous remettons particulièrement en cause les questions qui obligent l'auteur d'une demande de congé à fournir des renseignements personnels au sujet d'une autre personne.

Nous avons conclu que la plaignante avait dû fournir plus de renseignements personnels que nécessaire afin de faire la preuve qu'elle avait droit au congé, et nous avons confirmé que sa plainte était ***fondée***.

Nous avons aussi recommandé un ensemble de mesures pouvant être prises par Postes Canada pour aborder les préoccupations relatives à la protection de la vie privée.

L'organisation a accepté de mettre en place certaines des recommandations, notamment de recueillir seulement les renseignements personnels qui sont absolument nécessaires pour l'administration adéquate du programme. Postes Canada a indiqué, par exemple, qu'elle ne demanderait plus à connaître le nom des autres personnes (des tiers) qui auraient été associés aux soins donnés à la personne malade.

L'organisation a aussi accepté de mettre à jour les directives écrites que les superviseurs doivent suivre lors de la réception d'une demande de congé de la part d'un employé, de façon à veiller à ce que seuls les renseignements requis soient recueillis.

L'organisation souhaite toutefois continuer de recueillir des renseignements sur les autres membres de la famille qui travaillent à Postes Canada, afin de s'assurer qu'un seul employé demande congé pour prendre soin d'une personne pour éviter les abus.

En l'absence de preuves indiquant des abus répandus, nous continuons d'avoir des réserves quant à cette collecte de données. Nous avons invité l'organisation à trouver des façons moins intrusives pour la vie privée de prévenir la fraude au moment d'examiner les demandes de congé.

2.4.2 LE PERMIS DE CONDUIRE EST UN DOCUMENT D'IDENTITÉ ACCEPTABLE POUR LA LOCATION D'UNE CASE POSTALE

Une personne a présenté une plainte après que Postes Canada ait exigé qu'elle fournisse son numéro de permis de conduire afin de mettre fin à la location de sa case postale.

Postes Canada a fait valoir qu'elle devait demander aux personnes qui louent une case postale de fournir une pièce d'identité afin de veiller à ce que les cases ne soient pas utilisées ou réglées frauduleusement. La société d'État a aussi mentionné avoir déjà utilisé les renseignements recueillis pour enquêter sur des allégations d'envoi de biens illégaux à des cases postales louées.

Notre enquête nous a permis de déterminer que Postes Canada est légalement tenue d'assurer la sécurité du service postal et qu'elle recueille et utilise des renseignements personnels sur ses clients à des fins conformes à l'accomplissement de ce mandat. Nous avons déterminé que la saisie du numéro de permis de conduire et d'autres numéros d'identification est raisonnable et que la plainte était ***non fondée***.

2.5 Suivi de la vérification sur les fichiers inconsultables de la GRC

2.5.1 CONTEXTE

La *Loi sur la protection des renseignements personnels* confère aux personnes un droit général d'accès aux renseignements personnels qui les concernent et qui sont détenus par les institutions fédérales. Ce droit s'accompagne toutefois de restrictions précises.

Par exemple, l'article 18 de la *Loi* permet à certaines institutions de créer des fichiers inconsultables, qui contiennent habituellement des renseignements de nature très délicate liés à la sécurité nationale et à la criminalité.

Les personnes n'ont pas accès aux renseignements personnels les concernant qui sont conservés dans ces fichiers; en fait, elles ne peuvent même pas savoir que des renseignements les concernant s'y trouvent.

La nature spéciale et généralement secrète des activités liées à la sécurité et au renseignement peuvent justifier le fait que certains fichiers ne puissent pas être consultés par les membres du public. Nous reconnaissons bien sûr l'importance de garantir aux partenaires des milieux de l'application de la loi et de la sécurité, tant à l'échelle

nationale qu'internationale, que les renseignements communiqués à titre confidentiel seront protégés comme il se doit.

Toutefois, en échange du privilège de conserver des renseignements qui ne peuvent absolument pas être consultés par les membres du public, les institutions doivent veiller à ce que les fichiers inconsultables ne contiennent que des renseignements qui devraient légitimement s'y trouver. Comme le commissaire à la protection de la vie privée l'a fait remarquer en 1990 : « Il ne faudrait surtout pas qu'après avoir autorisé la création d'un fichier pareil, on lui permette de devenir, sans contrôle, un dépôt secret de renseignements personnels[2]. »

Il en est ainsi parce que les personnes dont le nom apparaît dans les fichiers inconsultables pourraient subir des conséquences défavorables. Par exemple, le nom d'une personne pourrait se trouver dans un fichier inconsultable simplement parce qu'elle se trouvait au mauvais endroit au mauvais moment, et qu'elle discutait avec la mauvaise personne. Il peut aussi arriver que certains renseignements communiqués par un informateur mal informé, ou motivé par d'autres facteurs que sa responsabilité civique, figurent dans un fichier inconsultable.

Si des renseignements erronés figurent dans un fichier inconsultable, il pourrait arriver que des personnes tout à faire innocentes aient de la difficulté à obtenir une autorisation de sécurité pour un emploi ou à franchir une frontière. Puisque le contenu des fichiers inconsultables demeure un secret, ces personnes pourraient ne jamais connaître l'origine de leurs difficultés.

Il importe donc de veiller à ce que les renseignements conservés dans les fichiers inconsultables fassent l'objet d'un examen continu afin de s'assurer qu'ils doivent bien s'y trouver.

Nous avons réalisé une vérification des fichiers inconsultables de la GRC en février 2008. Nous avons conclu que les fichiers n'étaient pas suffisamment bien gérés puisque des dizaines de milliers d'entre eux n'auraient pas dû en faire partie.

2.5.2 VÉRIFICATION DE SUIVI

Nous avons effectué, en 2010-2011, un suivi de la vérification de 2008 afin de déterminer si la GRC avait respecté les engagements qu'elle avait pris relativement à nos recommandations.

---

[2] Rapport annuel 1989-1990 du commissaire à la protection de la vie privée, p. 34.

Les responsables nous ont indiqué qu'à la suite de notre vérification, ils avaient procédé à un nouvel examen de tous les renseignements contenus dans les fichiers inconsultables de l'organisation et que cette initiative avait donné des résultats remarquables.

En mars 2008, le nombre de fichiers inconsultables liés à la sécurité nationale s'élevait à 5 288. En mars 2011, la majorité des fichiers avaient été retirés et il n'en restait que 190.

L'examen des fichiers de renseignement criminel a permis d'obtenir un résultat semblable. À la fin du dernier exercice, le nombre de fichiers inconsultables s'élevait à 2 898. Cela représente 58 379 fichiers de moins qu'il y a trois ans.

Selon la GRC, plus de 95 % des fichiers qui ont fait l'objet d'un nouvel examen ont été retirés des fichiers inconsultables liés à la sécurité nationale et au renseignement criminel.

La GRC a aussi affirmé avoir mis en place des mesures en réponse aux autres recommandations de notre vérification, notamment :

- ***une nouvelle structure de reddition de comptes intégrée a été mise en place pour la gestion des fichiers inconsultables, et des pouvoirs ont été délégués à des personnes précises pour l'approbation des fichiers à inclure;***
- ***un mécanisme d'examen centralisé a été mis en place afin de veiller à ce que le statut exact des fichiers soit indiqué dans les outils informatisés et sur les copies papier;***
- ***un cycle d'examen interne d'une durée de deux ans a été établi pour les fichiers inconsultables.***

Les nouvelles mesures visant à donner suite aux conclusions de la vérification devraient fournir un cadre permettant de veiller à ce que les renseignements détenus dans les fichiers inconsultables de la GRC respectent les exigences de la *Loi sur la protection des renseignements personnels* et de la politique interne connexe sur les fichiers inconsultables.

2.6 Intégration de la protection de la vie privée aux initiatives touchant la sécurité publique

Une nouvelle génération d'appareils mobiles, de capteurs de télédétection, de caméras à haute résolution et de logiciels analytiques a révolutionné les pratiques de surveillance et a grandement facilité la collecte, le traitement et la communication de l'information à l'échelle mondiale.

Ces outils permettent aux services de police et aux enquêteurs du gouvernement d'assurer la sécurité publique. Cela dit, l'accumulation non contrôlée de données sur les mouvements, les activités et les communications des citoyens peut également avoir des conséquences négatives en limitant le droit fondamental des citoyens de mener leurs activités de façon anonyme et sans faire l'objet d'une surveillance de la part de l'État.

L'intrusion injustifiée de la vie personnelle des citoyens est aux antipodes d'un État sécuritaire et confiant. Des mécanismes de contrôle ont été expressément mis au point afin d'assurer la protection d'un espace social plus vaste où les citoyens peuvent profiter de leur vie privée et se livrer à leurs activités personnelles en toute liberté.

2.6.1 DOCUMENT DE RÉFÉRENCE

Le Commissariat a tiré profit des conseils d'experts de la protection de la vie privée et de la sécurité au sein du milieu universitaire, de la communauté juridique, de la société civile ainsi que des secteurs politique, du renseignement, de l'application de la loi et de la surveillance afin d'élaborer un document de référence susceptible d'aider les responsables de l'élaboration des politiques, les praticiens et les citoyens à mieux comprendre ces enjeux complexes.

Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle

Le document, intitulé *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*, offre un cadre d'analyse clair et pratique pour l'intégration de mesures de protection de la vie privée aux nouveaux objectifs de sécurité publique et nationale, ainsi que les étapes à suivre pour parvenir à un juste équilibre.

2.6.2 LOI SUR L'ACCÈS LÉGAL

Les commissaires à la protection de la vie privée du Canada ont aussi continué d'exhorter les législateurs du gouvernement fédéral à faire preuve de prudence dans leurs efforts pour rééquilibrer les mesures de protection juridiques et les seuils en ce qui a trait à l'accès, par le gouvernement, à des renseignements personnels.

En mars 2011, la commissaire à la protection de la vie privée Jennifer Stoddart et tous les commissaires à la protection de la vie privée provinciaux et territoriaux ont écrit au sous-ministre de Sécurité publique Canada afin de lui faire part des risques pour la vie privée qui pourraient découler de l'intention du gouvernement de modifier le régime légal régissant sur des outils électroniques de fouille, de saisie et de surveillance.

Le Commissariat continue de faire valoir qu'il n'existe pas suffisamment de données pour justifier les nouveaux pouvoirs accrus d'accès légal, que d'autres solutions moins envahissantes peuvent être étudiées et que les mesures de surveillance de l'accès légal devraient être renforcées.

2.7 Introduction à la biométrie

2.7.1 CONTEXTE

Pour bon nombre d'interactions avec l'État, les personnes n'ont d'autre choix que de fournir des renseignements personnels, souvent de nature délicate, en grande quantité. Pour obtenir un passeport, par exemple, les personnes doivent fournir des renseignements au sujet de leur lieu de résidence et de leur profession, et consentir à l'utilisation d'une image faciale.

Les renseignements personnels constituent habituellement la monnaie d'échange utilisée pour l'accès à des programmes, à des services ou à des prestations du gouvernement.

Le Commissariat a remarqué que les organismes gouvernementaux s'intéressent de plus en plus à l'utilisation d'outils biométriques pour gérer l'accès aux programmes et aux services. Le terme « biométrie » désigne un éventail de techniques, d'appareils et de systèmes qui permettent à des machines de reconnaître des personnes, ou de confirmer ou d'authentifier leur identité.

De tels outils mesurent et analysent les caractéristiques physiques et comportementales des personnes, comme la démarche, les traits du visage, l'empreinte vocale, les empreintes digitales, les empreintes palmaires, les dessins des veines du doigt ou de la paume, ou la structure de l'œil (iris ou rétine).

Les données biométriques sont recueillies à un point de départ. L'identité d'une personne peut par la suite être établie ou authentifiée lorsque de nouvelles données sont recueillies et comparées avec les données qui figurent déjà dans le système.

L'exemple le plus courant de l'application de la biométrie est celui de l'utilisation d'une photographie dans un passeport, sur un permis de conduire ou sur une carte d'assurance-maladie. L'image faciale d'une personne est saisie et conservée, de façon à pouvoir plus tard être comparée avec une autre photographie ou avec la personne elle-même.

2.7.2 DÉFIS POUR LA PROTECTION DE LA VIE PRIVÉE

D'un côté, la technologie biométrique peut contribuer à la mise en place de systèmes d'identification très robustes et très fiables — plus fiables, par exemple, que les systèmes fondés sur des registres papier.

De l'autre, elle peut aussi poser des risques importants pour la vie privée associés à la collecte dissimulée de caractéristiques biométriques, au recoupement et à la divulgation non intentionnelle de renseignements secondaires intégrés dans le profil biométrique d'une personne.

Un grand nombre de renseignements biométriques, comme les empreintes digitales et les images faciales, peuvent en outre être recueillis sans qu'une personne le sache ou y consente. Ils peuvent, par conséquent, être utilisés de façon dissimulée afin de surveiller et de suivre les déplacements et les comportements d'une personne.

Il est crucial, pour toutes ces raisons, que les institutions fédérales et les autres organisations y réfléchissent à deux fois avant de proposer la mise en œuvre d'initiatives nécessitant la collecte de renseignements biométriques.

Afin de faciliter cette analyse, le Commissariat a élaboré un document d'introduction détaillé qui porte sur les avantages et les inconvénients de la biométrie. Ce document, qui a été publié en 2010-2011, est intitulé *Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée*.

Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée

Le document d'introduction contient des renseignements de base sur la biométrie et sur les systèmes qui utilisent des données biométriques. Il fait aussi état de certaines des répercussions pour la vie privée qui découlent de cette nouvelle technologie et des mesures qui peuvent être prises afin d'atténuer les risques.

Cette publication, qui se trouve sur notre site Web, présente une méthode qui permet de déterminer s'il convient d'utiliser des renseignements biométriques à des fins données et formule des recommandations pour la conception d'outils qui tiennent compte des considérations relatives à la protection de la vie privée.

Comme l'explique le document d'introduction, le défi que les organisations doivent relever consiste à concevoir, à mettre en œuvre et à exploiter des systèmes qui permettent d'améliorer les services d'identification sans pour autant compromettre de façon indue la protection de la vie privée.

CHAPITRE 3

La conservation des données

Le gouvernement fédéral utilise-t-il les renseignements personnels à bon escient?

À l'été 2010, WikiLeaks a surpris le monde entier en publiant des documents de l'armée américaine classifiés sur la guerre en Afghanistan. Cette révélation a été suivie, quelques mois plus tard, de la publication de documents sur la guerre en Iraq et de la divulgation massive de messages échangés entre le département d'État américain et ses missions à l'étranger.

La communication sans précédent de renseignements militaires et gouvernementaux de nature délicate en ligne et dans les médias grand public a suscité une foule de débats sur des questions allant de la liberté de presse et de la transparence gouvernementale à la sécurité des données et à la politique étrangère américaine.

L'axiome selon lequel l'information est le pouvoir s'est encore une fois vérifié. L'État possède généralement beaucoup de pouvoir et le citoyen relativement peu; la divulgation de tous ces documents a été vue comme la tentative d'une organisation non gouvernementale de rééquilibrer les choses.

Sans égard au bien-fondé des fuites d'information de WikiLeaks, il faut admettre que les sociétés occidentales ont toujours cherché des façons d'obliger les gouvernements à rendre des comptes à la population. Or, la façon dont le gouvernement gère l'information est l'un des principaux éléments de la reddition de comptes.

Dans un monde idéal, un gouvernement responsable serait totalement transparent tout en protégeant la confidentialité des renseignements personnels de ses citoyens.

Au cours de la dernière année, le Commissariat a parlé aux parlementaires de l'importance d'un gouvernement transparent. Nous avons affirmé que cela n'est pas

contraire à l'obligation du gouvernement de protéger la vie privée des personnes en vertu de la *Loi sur la protection des renseignements personnels*.

Comme l'explique le chapitre précédent, la *Loi* prévoit que les renseignements personnels doivent être recueillis, conservés et éliminés de façon appropriée. Le chapitre qui suit décrit aussi l'importance des mesures de protection contre la communication inappropriée de renseignements personnels.

UTILISATIONS APPROPRIÉES

Mais il y a plus. La *Loi sur la protection des renseignements personnels* oblige aussi le gouvernement à utiliser les renseignements personnels des citoyens à des fins définies et appropriées. Par exemple, il est approprié d'utiliser des renseignements liés aux revenus pour la gestion d'un avantage fiscal.

Ce n'est toutefois pas approprié d'utiliser les renseignements personnels d'un homme qui a été membre de nos forces armées pour préparer une note d'information à l'intention du ministre des Anciens Combattants concernant la participation de cet homme à une conférence de presse sur la Colline parlementaire au sujet d'enjeux relatifs aux anciens combattants.

Utilisation des renseignements personnels

À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci : a) *qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins.*

— Loi sur la protection des renseignements personnels, article 7

À l'exception de certains types de données qui sont expressément exclues des dispositions de la *Loi*, cette dernière permet aux personnes d'avoir accès aux renseignements personnels qui les concernent et qui sont détenus par le gouvernement. Sans cet accès, les personnes n'auraient aucun moyen de savoir si les renseignements détenus à leur sujet par le gouvernement sont exacts ou exhaustifs.

Ce chapitre porte sur les bonnes et les mauvaises utilisations des renseignements personnels par le gouvernement du Canada en 2010-2011. Il aborde les questions relatives à l'accès aux renseignements personnels et se termine par une discussion sur la protection de la vie privée dans le contexte d'un gouvernement plus ouvert et plus transparent.

3.1 Atteinte à la vie privée par Anciens Combattants Canada

L'ENQUÊTE CONCLUT QUE LES RENSEIGNEMENTS PERSONNELS D'UN ANCIEN COMBATTANT ONT ÉTÉ TRAITÉS DE FAÇON GRAVEMENT INAPPROPRIÉE.

3.1.1 APERÇU

L'enquête menée au sujet d'une plainte importante déposée par un ancien militaire a soulevé d'importantes inquiétudes au sujet de la gestion des renseignements personnels médicaux de nature délicate et d'autres renseignements personnels par Anciens Combattants Canada. L'absence apparente de mécanismes de contrôle visant à éviter que des renseignements personnels de nature délicate puissent être consultés par un grand nombre de personnes et diffusés au sein du Ministère nous a particulièrement inquiétés.

Cette enquête a révélé l'existence de graves problèmes systémiques, ce qui nous a incités à annoncer la tenue d'une vérification de la conformité du Ministère à la *Loi sur la protection des renseignements personnels*. Nous avons, depuis ce temps, reçu d'autres plaintes.

Dans cette première plainte, l'ancien combattant alléguait que le Ministère avait enfreint la *Loi sur la protection des renseignements personnels* en utilisant ses renseignements personnels de façon inappropriée lorsqu'il a fait état, de façon excessivement détaillée, de renseignements médicaux, financiers et autres renseignements personnels de nature délicate dans des notes d'information à l'intention du ministre des Anciens Combattants. Le plaignant alléguait aussi que le Ministère avait transmis son dossier médical à un hôpital administré par Anciens Combattants, et cela, sans son consentement.

Les incidents mentionnés dans la plainte sont survenus en 2005 et en 2006. Nous avons transmis un résumé des conclusions de notre enquête et de nos recommandations au Ministère en octobre 2010. La vérification du Ministère est en cours et nous nous attendons à ce qu'elle soit terminée à l'hiver 2012.

3.1.2 NOTES D'INFORMATION MINISTÉRIELLES

Notre enquête nous a permis de confirmer que plusieurs notes d'information rédigées à l'intention du ministre des Anciens Combattants de l'époque contenaient des renseignements personnels au sujet du plaignant. La quantité de renseignements personnels et leur nature délicate, y compris des renseignements médicaux et financiers, contenus dans deux notes d'information à l'intention du ministre étaient excessives et allaient au-delà de ce qui était nécessaire aux fins visées.

Les notes faisaient notamment état de nombreux détails sur les interactions du plaignant avec le Ministère, tant à titre de client que de défenseur des droits des anciens combattants. Nous avons été particulièrement inquiétés par une note rédigée en mars 2006 afin de communiquer au ministre de l'information sur la participation du plaignant à une conférence de presse tenue sur la colline du Parlement afin de discuter de questions liées aux anciens combattants.

En plus de fournir au ministre de l'information sur les activités menées par le plaignant pour défendre les droits des anciens combattants, la note renfermait des renseignements de nature délicate au sujet du plaignant : diagnostic médical, symptômes, pronostic, fréquence des rendez-vous médicaux, plans de traitement recommandés, historique des interactions du plaignant avec le Ministère et montant des prestations reçues. Tous ces renseignements avaient été fournis au Ministère par le plaignant lorsque celui-ci avait présenté une demande en vue d'obtenir des prestations à titre d'ancien combattant.

Nous avons par ailleurs trouvé inquiétante la façon dont les renseignements personnels du plaignant avaient été communiqués à de nombreuses personnes au sein du ministère des Anciens Combattants, y compris à des employés de la Politique sur les programmes, des Communications et des Relations avec les médias, lors de l'élaboration des notes d'information. Des renseignements personnels de nature délicate ont été communiqués à des fonctionnaires qui devraient normalement avoir peu ou pas besoin de les connaître pour accomplir leurs fonctions.

3.1.3 TRANSMISSION DE DONNÉES PERSONNELLES À UN HÔPITAL

En ce qui concerne la deuxième question soulevée par la plainte, l'enquête a permis de déterminer que le Ministère avait transmis de grandes quantités de renseignements personnels et médicaux concernant le plaignant à un hôpital qu'il administrait. Les renseignements communiqués comprenaient des rapports médicaux, des lettres échangées entre le plaignant et le Ministère, ainsi qu'une note d'information à l'intention du ministre.

Le ministère des Anciens Combattants a indiqué qu'il avait transmis les renseignements à l'hôpital afin de déterminer si le plaignant satisfaisait aux critères établis pour participer à un programme de traitement qui y était offert.

Les directives ministérielles prévoient que les clients doivent autoriser la transmission de tels renseignements par écrit. Cela n'a toutefois pas eu lieu.

3.1.4 CONCLUSIONS

En ce qui concerne les deux questions soulevées dans la plainte, l'enquête a conclu que l'utilisation, par le ministère des Anciens Combattants, des renseignements personnels et médicaux du plaignant était contraire à l'article 7 de la *Loi*. Celle-ci indique que les renseignements personnels détenus par un ministère ne doivent pas être utilisés par celui-ci sans le consentement de la personne visée à des fins autres que celles auxquelles ils ont été recueillis ou préparés ou pour les usages qui sont compatibles à ces fins.

Par conséquent, nous avons conclu que la plainte était ***fondée***.

3.1.5 RECOMMANDATIONS

La commissaire adjointe a présenté à Anciens Combattants Canada les recommandations suivantes :

- ***Entreprendre immédiatement l'élaboration d'un cadre amélioré de protection des renseignements personnels ainsi que des mesures de protection et des contrôles adéquats visant à restreindre l'accès aux renseignements personnels au sein du Ministère.***
- ***Revoir les politiques et les pratiques de gestion de l'information en place afin de s'assurer que les renseignements personnels ne sont communiqués qu'aux employés du Ministère qui en ont véritablement besoin.***
- ***Offrir aux employés une formation sur le traitement approprié des renseignements personnels.***
- ***Examiner les procédures afin de s'assurer que le consentement est obtenu de la personne avant le transfert des renseignements la concernant à d'autres institutions.***

3.1.6 RÉPONSE DU MINISTÈRE

À la suite de la publication des conclusions de notre enquête, le Ministère a amorcé la mise en œuvre d'un plan d'action en dix points visant à répondre à nos préoccupations. Le Ministère a indiqué qu'avant la fin de l'exercice, il avait nommé des experts externes des systèmes d'information électroniques et de la protection de la vie privée, et qu'il effectuait un suivi proactif de l'accès des employés aux renseignements des clients et menait des enquêtes au besoin.

Le ministère des Anciens Combattants a aussi indiqué qu'il donnait à ses employés une formation obligatoire sur la protection de la vie privée et qu'il avait mis en place de nouvelles procédures sur l'utilisation appropriée des renseignements des clients dans les notes d'information et les autres documents ministériels. Les employés ont aussi été avisés qu'une politique sur la discipline plus stricte avait été élaborée et que des sanctions claires étaient prévues en cas d'infraction.

À plus long terme, le Ministère s'est engagé à procéder à des évaluations annuelles indépendantes afin d'assurer la conformité à la *Loi sur la protection des renseignements personnels*.

3.1.7 VÉRIFICATION DE LA CONFORMITÉ À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Au moment de notre enquête, nous avons constaté que les fonctionnaires d'Anciens Combattants Canada étaient incapables de nommer ou d'expliquer clairement les politiques, les procédures ou les pratiques habituelles en matière de communication de renseignements. Nous n'étions donc pas convaincus que le Ministère avait mis en place des politiques et des procédures en vue du traitement approprié des renseignements personnels des anciens combattants.

Par conséquent, nous avons annoncé la tenue d'une vérification afin de déterminer si le Ministère avait donné suite aux recommandations formulées afin de pallier les lacunes cernées lors de notre enquête. Nous voulions aussi savoir si le plan d'action en dix points permettait la mise en place des politiques, des procédures et des processus nécessaires à la gestion des renseignements personnels d'une façon conforme à la *Loi sur la protection des renseignements personnels*.

Nous prévoyons présenter les résultats de notre vérification à l'hiver 2012.

3.2 Autres enquêtes sur des plaintes liées à l'utilisation de renseignements personnels

3.2.1 UN FACTEUR ACCUSE SA SUPERVISEURE D'AVOIR INTERCEPTÉ ET LU UN DOCUMENT

Un facteur de Postes Canada a déposé une plainte dans laquelle il alléguait que sa superviseure avait pris connaissance, sans permission, du contenu d'un formulaire médical concernant une demande d'assurance invalidité.

Le plaignant a indiqué avoir remis le formulaire dans une enveloppe scellée à sa superviseure, supposant que celle-ci l'acheminerait, sans l'ouvrir, à la compagnie d'assurance médicale. Le facteur a affirmé que la superviseure avait ouvert l'enveloppe, avait pris connaissance du contenu du formulaire, et s'était servi des renseignements qui y figuraient afin de mettre en doute la validité d'autres documents médicaux qu'il avait présentés à Postes Canada.

Lors de notre enquête, la superviseure a reconnu qu'elle avait peut-être pris connaissance du contenu du formulaire, mais qu'elle ne se rappelait pas l'avoir fait. Elle a toutefois insisté sur le fait qu'elle n'aurait jamais ouvert une enveloppe scellée.

Notre enquête ne nous a pas permis de déterminer si le formulaire avait véritablement été remis dans une enveloppe scellée. Nous avons toutefois pu confirmer que la superviseure s'était servi des renseignements sur l'état de santé qui figuraient dans le formulaire afin de contredire le contenu d'autres documents médicaux présentés par l'employé.

Nous avons conclu que les renseignements personnels de l'employé avaient bel et bien été utilisés à une fin qui ne correspondait pas à celle pour laquelle ils avaient été recueillis, et qu'ils avaient été utilisés à cette fin sans la permission du plaignant. Nous avons donc conclu que la plainte était ***fondée***.

Nous avons cependant constaté qu'il s'agissait d'un cas isolé et que Postes Canada avait mis en place des pratiques claires pour la gestion des demandes d'assurance invalidité.

Nous avons recommandé que Postes Canada rappelle à tous ses employés de présenter leurs formulaires de réclamation directement à l'assureur. Nous avons aussi recommandé que l'organisation rappelle aux gestionnaires de refuser d'acheminer de tels formulaires au nom de leurs employés.

3.2.2 UN PROGRAMME D'EMBAUCHE D'ANCIENS MILITAIRES UTILISE DES RENSEIGNEMENTS PERSONNELS À BON ESCIENT

Une personne s'est plainte au Commissariat du fait que la Commission de la fonction publique du Canada avait recueilli et communiqué, de façon inappropriée, des renseignements personnels au sujet de sa libération des Forces armées canadiennes pour des raisons médicales.

Les renseignements avaient été recueillis aux fins d'un programme dans le cadre duquel les candidatures d'anciens militaires sont étudiées en priorité en vue de pourvoir des postes vacants au sein de la fonction publique fédérale.

Notre enquête a permis de déterminer que tous les aspects du processus étaient pleinement conformes aux dispositions de la *Loi sur la protection des renseignements personnels*. Nous avons en effet constaté que le plaignant avait consenti par écrit à la collecte et à la communication de renseignements sur sa libération de l'armée pour des raisons médicales aux fins du programme d'embauche prioritaire.

Par conséquent, nous avons conclu que la plainte n'était ***pas fondée***.

3.3 Enquête sur des plaintes concernant l'accès à des renseignements personnels

3.3.1 SANTÉ CANADA A EU TORT DE REFUSER L'ACCÈS À DES RENSEIGNEMENTS PERSONNELS

Une personne a présenté une plainte au Commissariat après que Santé Canada ait refusé de lui donner accès à des renseignements personnels qui avaient été recueillis à son sujet avant, pendant et après l'évaluation de son aptitude au travail. L'évaluation avait été réalisée dans le cadre d'un programme de Santé Canada sur la santé et la sécurité en milieu de travail.

Le Ministère a refusé de communiquer l'information invoquant l'article 28 de la *Loi sur la protection des renseignements personnels*. Cet article prévoit que le responsable d'un ministère peut refuser de communiquer des renseignements personnels liés l'état physique ou mental d'une personne dans le cas où la prise de connaissance des renseignements qui y figurent desservirait celle-ci

Les dispositions réglementaires prévoient en outre que le responsable de l'institution peut montrer les renseignements personnels à un médecin praticien ou à un psychologue

qui possède les compétences nécessaires pour déterminer si la communication de l'information desservirait la personne concernée. Le recours à un professionnel de la médecine nécessite toutefois le consentement de la personne visée.

Après enquête, nous avons conclu que les renseignements personnels que le plaignant souhaitait obtenir ne se limitaient pas à des renseignements de nature délicate liés à son état mental ou physique. Nous avons donc conclu que l'article 28 de la *Loi* ne donnait pas à Santé Canada le droit de refuser l'accès aux renseignements personnels.

Par conséquent, nous avons conclu que la plainte était ***fondée***. Puisque le Ministère a décidé de communiquer l'information demandée, nous avons aussi déterminé que le dossier était ***résolu***.

3.4 Travail juridique en faveur de l'accès aux renseignements personnels

En vertu de l'article 41 de la *Loi sur la protection des renseignements personnels*, les personnes qui se sont vu refuser l'accès aux renseignements personnels les concernant détenus par une institution fédérale peuvent présenter une demande d'audience devant la Cour fédérale en vue d'un examen du refus.

En vertu de l'article 42 de la Loi, la commissaire peut également présenter une demande d'audience devant la Cour en vue de l'examen du refus d'accorder à une personne l'accès à des renseignements personnels la concernant.

La *Loi* ne permet pas actuellement à une personne ou à la commissaire de présenter une demande d'audience pour d'autres infractions à la *Loi*, comme la collecte, l'utilisation ou la communication injustifiée de renseignements personnels par une institution fédérale. Au fil des années, le Commissariat a souvent recommandé que le gouvernement fédéral élargisse les motifs pour lesquels une demande en vertu de la *Loi* peut être présentée à la Cour fédérale.

Vous trouverez ci-dessous une demande présentée à la Cour à laquelle nous avons participé en 2010-2011. Conformément à l'esprit de notre mandat, nous n'indiquons pas le nom des demandeurs. En revanche, nous fournissons les numéros de dossier de la Cour ainsi que le nom des institutions mises en cause, le cas échéant.

3.4.1 *X. c. COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA* Nº DE DOSSIER DE LA COUR FÉDÉRALE : T-555-10

Il s'agit d'une demande de contrôle judiciaire qui a été présentée à l'endroit de la commissaire à la protection de la vie privée, et dans laquelle le plaignant demande qu'une ordonnance soit rendue afin d'obliger le Commissariat à mener une nouvelle enquête sur une plainte qu'il a présentée contre le Conseil de recherches en sciences humaines (CRSH) au sujet d'un refus de communication de renseignements personnels le concernant en vertu de la *Loi sur la protection des renseignements personnels*. Le demandeur allègue que le Commissariat à la protection de la vie privée n'a pas effectué une enquête en règle sur sa plainte et qu'il avait un parti pris.

Le Commissariat se défend contre cette demande. Après un certain nombre de questions interlocutoires, il a été décidé que l'affaire serait entendue les 6 et 7 septembre 2011.

3.5 Transparence gouvernementale

Le principe de la transparence gouvernementale prévoit que les affaires du gouvernement devraient être transparentes, à tous les niveaux, afin de permettre la pleine participation des citoyens ainsi qu'un examen et une surveillance efficaces de la part du public.

Le Commissariat appuie le principe de la transparence gouvernementale en tant que principe clé de la démocratie et que pierre d'assise de la relation de confiance entre le gouvernement et les citoyens.

Nous croyons cependant que la transparence ne devrait pas avoir lieu aux dépens du droit des personnes à la vie privée conféré par la loi. La confiance des citoyens envers le gouvernement repose aussi sur l'assurance que celui-ci traitera les renseignements personnels de ces derniers avec respect, qu'il les protégera et qu'il veillera à ce qu'ils ne soient pas communiqués de manière inappropriée.

En 2010-2011, nous avons fait valoir la nécessité d'assurer cet équilibre sur plusieurs tribunes, y compris dans une lettre, en juillet 2010, à l'intention du Comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique (ETHI).

Deux mois plus tard, les commissaires à l'accès à l'information et à la protection de la vie privée des gouvernements fédéral, provinciaux et territoriaux ont signé une résolution

visant à appuyer et à promouvoir le gouvernement ouvert en tant que moyen d'accroître la transparence et la reddition de comptes. La résolution précisait qu'un gouvernement ouvert doit accorder toute l'attention voulue à la protection de la vie privée, à la confidentialité et à la sécurité.

À la mi-février 2011, la commissaire adjointe, Chantal Bernier, a comparu devant le Comité ETHI afin de discuter plus à fond des enjeux.

Elle a indiqué que la ligne qui sépare les renseignements qui permettent d'identifier une personne de ceux qui ne le permettent pas est de plus en plus floue en raison des nouvelles technologies de l'information. Les renseignements qui semblent, à première vue, anonymes ou dépersonnalisés peuvent, dans certains cas, être combinés à des données provenant d'autres sources et permettre d'établir des liens avec des personnes.

Si des données contiennent des renseignements concernant une personne identifiable, toutes les exigences et les mesures de protection prévues dans la *Loi sur la protection des renseignements personnels* doivent être respectées.

Les autorités chargées de la protection des données, ici et partout dans le monde, sont de plus en plus convaincues que les gouvernements doivent incorporer les considérations relatives à la protection de la vie privée directement lors de la conception des programmes et services dans le cadre desquels des données personnelles seront recueillies. La protection de la vie privée doit être une valeur par défaut, et non pas un élément qu'on ajoute après coup.

Au niveau opérationnel, il est essentiel de prêter attention à la formation continue des employés sur la protection de la vie privée, aux règles et aux procédures appropriées de communication de l'information, ainsi qu'aux rouages et au renouvellement des systèmes d'accès à l'information et de protection des renseignements personnels.

3.6 Demandes présentées au CPVP en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*

Le Commissariat à la protection de la vie privée du Canada est assujetti à la *Loi sur l'accès à l'information* et à la *Loi sur la protection des renseignements personnels*. Voici un sommaire de nos activités en vertu de ces deux lois au cours du dernier exercice.

3.6.1 *LOI SUR L'ACCÈS À L'INFORMATION*

En 2010-2011, le Commissariat a reçu 63 nouvelles demandes en vertu de *la Loi sur l'accès à l'information* en vue de la communication de documents gouvernementaux dont il a la garde, ce qui représente 11 demandes de plus que l'année précédente. Une demande de 2010-2011 a été reportée de l'exercice précédent. Au total, 31 demandes d'accès à l'information reçues au cours du dernier exercice visaient la communication de documents détenus par d'autres institutions fédérales et ont par conséquent été réacheminées à ces dernières.

Nous avons répondu à 64 demandes d'accès à l'information avant la fin de l'exercice, et une de ces demandes a été reportée.

Nous avons été informés qu'une plainte avait été présentée à la commissaire à l'information du Canada en vertu de la *Loi sur l'accès à l'information* en 2010-2011, comparativement à deux pour l'exercice précédent. Cette nouvelle plainte alléguait un refus d'accès à des documents du gouvernement. Le Commissariat à l'information a déterminé qu'elle n'était pas fondée.

3.6.2 *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

En 2010-2011, nous avons reçu 105 demandes en vertu de la *Loi sur la protection des renseignements personnels* pour de l'information personnelle contenue dans des documents en notre possession et nous en avons fermé 106. En comparaison, nous avions reçu 61 demandes lors de l'exercice financier de 2009-2010 et en avions fermé 60.

Un total de 91 demandes de renseignements personnels reçues en 2010-2011 portait sur des documents détenus par d'autres institutions fédérales; ces demandes ont donc été redirigées.

Nous avons reçu cinq plaintes en vertu de la *Loi sur la protection des renseignements personnels* durant l'exercice financier, dont quatre provenaient de la même personne. Une plainte portait sur les délais liés à l'accès aux renseignements personnels, une autre était liée aux exceptions invoquées pour ne pas fournir les documents, et trois portaient sur des documents égarés.

Ces plaintes ont été transférées au commissaire spécial à la protection de la vie privée, dont le mandat est d'enquêter de façon indépendante sur toute plainte qui peut être déposée contre le Commissariat à la protection de la vie privée du Canada en vertu de la *Loi sur la protection des renseignements personnels.*

CHAPITRE 4

Trop généreux?

Comment le gouvernement communique les renseignements personnels

Quand il est question de la communication de leurs renseignements personnels, les Canadiennes et Canadiens s'attendent à ce que leur gouvernement soit avare, chiche et parcimonieux.

La *Loi sur la protection des renseignements personnels* exige des ministères et des organismes fédéraux qu'ils protègent les renseignements personnels des Canadiennes et Canadiens. Le gouvernement ne peut communiquer les renseignements personnels qu'il a en sa possession sans avoir obtenu l'autorisation de la personne touchée, sauf lorsque des exceptions précises s'appliquent.

Le gouvernement a pris des mesures pour renforcer sa gestion prudente des renseignements personnels en modernisant son infrastructure de gestion de l'information. Malheureusement, comme le décrit ce chapitre, une atteinte à la protection des renseignements personnels a assombri cette initiative à la fin de septembre 2010.

Outre les atteintes, lorsqu'il est question du partage délibéré des renseignements — que ce soit entre les ministères ou avec d'autres autorités nationales ou étrangères — le gouvernement doit faire preuve d'une grande discrétion. Les renseignements ne doivent être communiqués qu'au besoin seulement, et uniquement dans le but de satisfaire à l'objectif énoncé.

Le paragraphe 8(2) de la *Loi* établit les circonstances dans lesquelles les renseignements personnels peuvent être communiqués. Par exemple, pour aider un organisme d'enquête à faire respecter une loi fédérale ou provinciale, mais seulement si la demande précise le but et décrit l'information qui doit être communiquée. La *Loi* permet également la communication de renseignements personnels sans autorisation si le responsable d'une

institution croit que l'intérêt public à l'égard de cette information prime sur l'atteinte à la vie privée.

Au fil des années, les restrictions imposées par la *Loi* ont été définies davantage et renforcées par des directives du Conseil du Trésor. Par exemple, si des renseignements personnels doivent être communiqués à d'autres autorités, des ententes officielles de partage d'information doivent clairement établir qui peut voir ces renseignements et en vertu de quelles conditions.

Le but est d'empêcher que des renseignements personnels de nature délicate soient communiqués à des personnes non autorisées. Après tout, l'atteinte à la protection des renseignements personnels peut entraîner des répercussions pour les personnes touchées : embarras, inconvénients ou même vol d'identité avec les difficultés économiques qui en découlent souvent.

IMPORTANTES RÉPERCUSSIONS

Le besoin de protéger les renseignements personnels revêt une importance particulière lorsque les personnes n'ont pas le droit de voir ces renseignements et de les corriger en vertu de la *Loi sur la protection des renseignements personnels*, souvent parce que l'information est conservée dans des bases de données exclues des modalités d'accès prévues par la *Loi*.

À titre d'exemple, les personnes ne peuvent savoir quels renseignements sont détenus par les organismes responsables de la sécurité et elles ne peuvent voir ces renseignements ni les modifier.

Par conséquent, si des renseignements inexacts ou incomplets sont partagés avec d'autres autorités, les libertés de ces personnes pourraient être restreintes. Leurs noms pourraient être ajoutés par erreur à des listes de surveillance et on pourrait leur interdire de voyager à l'étranger. Dans des cas extrêmes, ces personnes pourraient même être emprisonnées ou déportées.

Outre les renseignements communiqués de façon inappropriée, il y a ceux qui font l'objet de fuites. Les atteintes à la protection des renseignements personnels peuvent être des actes délibérés de malfaisance ou alors de simples accidents ou oublis.

Certaines atteintes sont portées à notre attention lorsque la personne touchée dépose une plainte au Commissariat. Dans d'autres cas, le ministère ou l'organisme nous signale l'atteinte directement et nous précise les mesures prises pour en atténuer les répercussions.

La *Loi sur la protection des renseignements personnels* ne contient aucune exigence concernant le signalement des atteintes ni aucune sanction, mais la politique du Conseil du Trésor encourage fortement les institutions à nous avertir si des renseignements personnels en leur possession sont exposés de façon inappropriée.

Nous sommes heureux de mentionner que, contrairement aux autres années, il n'y a pas eu d'atteintes flagrantes à la protection des renseignements personnels en 2010-2011 touchant l'information personnelle de dizaines de milliers de personnes.

Toutefois, nous avons remarqué que l'erreur humaine continue d'être une cause importante des atteintes à la protection des renseignements personnels. Des dossiers et des cahiers ont été oubliés dans des autobus et des avions, des curriculum vitae ont été affichés en ligne par erreur et une liste de numéros d'assurance sociale a été laissée à la vue de tous.

Le présent chapitre fait état de nos enquêtes sur des plaintes portant sur la communication inappropriée de renseignements personnels, de même que des rapports sur les atteintes soumis au Commissariat.

On y décrit aussi l'évaluation des facteurs relatifs à la vie privée envoyée par la GRC à propos des nouvelles technologies de partage de données et on y résume les mesures prises par diverses institutions pour traiter des inquiétudes en matière de sécurité des renseignements que nous avons mentionnées dans des vérifications de la protection de la vie privée antérieures.

Enfin, le chapitre se termine avec une mise à jour des cas où les institutions nous ont avertis qu'elles avaient communiqué des renseignements personnels sans consentement, mais dans l'intérêt du public.

4.1 Enquêtes sur des plaintes portant sur la communication de renseignements personnels

4.1.1 UN INFIRMIER EN PSYCHIATRIE OUBLIE LE DOSSIER DE TRAITEMENT D'UN ANCIEN DÉTENU DANS L'AUTOBUS

Un ancien détenu du Centre correctionnel communautaire Keele de Toronto a porté plainte après qu'un infirmier en psychiatrie à l'emploi de l'institution ait oublié une enveloppe contenant de l'information sur ses traitements dans un autobus.

Le directeur du centre, qui est un foyer de transition pour 40 hommes libérés d'institutions fédérales en vertu de modalités de liberté d'office, a écrit au plaignant pour l'aviser de la perte des documents.

Le directeur a reconnu l'atteinte à la vie privée du plaignant et s'est excusé de l'incident. Il a aussi indiqué qu'une enquête avait été menée à l'interne et que des mesures avaient été prises pour éviter qu'une telle situation se répète.

Plus précisément, on a rappelé à l'infirmier qu'il avait la responsabilité de protéger les renseignements personnels des patients. On lui a également rappelé de ne pas sortir les dossiers des patients, sauf si l'information est cryptée.

Notre enquête a confirmé que la vie privée du plaignant avait été compromise et que sa plainte était ***fondée***.

Nous avons également conclu que l'institution, qui relève du Service correctionnel du Canada, avait pris les mesures correctives appropriées dans le cadre de l'incident.

4.1.2 UNE LISTE DE NUMÉROS D'ASSURANCE SOCIALE EST PERDUE

Une femme a déposé une plainte portant sur la mauvaise gestion de ses renseignements personnels lors d'une séance d'information pour les prestataires d'assurance-emploi. Ressources humaines et Développement des compétences Canada (RHDCC) tient ces séances d'information obligatoires essentiellement pour confirmer l'identité des prestataires, qui présentent habituellement des demandes de prestations en ligne, sans contact en personne.

À la fin de la séance, la prestataire a appris que la liste de présences avait disparu. On lui a dit que cette liste contenait le nom, le numéro de téléphone et le numéro d'assurance sociale des 32 participants à la séance.

Les responsables du Ministère ont préparé un rapport et ont informé le bureau d'accès à l'information et de protection des renseignements personnels, de même que le Commissariat, de l'incident. Ils ont aussi avisé toutes les personnes touchées, se sont excusés et leur ont fourni de l'information sur la façon de se protéger du vol d'identité.

L'enquête a révélé que le Ministère n'avait pas protégé les renseignements personnels imprimés sur la feuille de façon appropriée. Nous avons conclu que la plainte était ***fondée***.

Nous avons été particulièrement inquiets du fait que l'atteinte concernait des numéros d'assurance sociale, qui sont des renseignements personnels très importants pour les personnes traitant avec les institutions fédérales ou autres. En raison de leur valeur, ces numéros sont très susceptibles d'être utilisés à de mauvaises fins s'ils tombent entre les mains de voleurs d'identité.

Pire encore, RHDCC, le ministère chargé d'émettre les numéros d'assurance sociale et d'en gérer l'utilisation, était responsable de cette atteinte.

Toutefois, nous avons noté que les responsables de la région où l'incident est survenu ont pris toutes les mesures raisonnables pour atténuer les conséquences de l'atteinte et pour éviter qu'une telle situation se répète.

Entre autres, ils ont demandé aux responsables de masquer les numéros d'assurance sociale sur les listes de présence avant que les documents ne soient utilisés lors de séances d'information pour les prestataires d'assurance-emploi. On prévoit que cette pratique sera adoptée dans l'ensemble du pays.

4.1.3 LES SOUPÇONS D'UN MINISTRE À PROPOS DE FUITES PROVENANT DE LA COMMISSION CANADIENNE DU BLÉ NE SONT PAS FONDÉS

En novembre 2009, le ministre d'Agriculture et Agroalimentaire Canada, qui est également responsable de la Commission canadienne du blé (CCB), a déposé une plainte au Commissariat contre l'organisme de commercialisation du blé.

La plainte faisait suite à des reportages dans les médias sur une vérification interne menée par la CCB relativement au processus de carnets de livraison, qui permet de faire le suivi des ventes de grains des producteurs de l'Ouest canadien par l'intermédiaire de la CCB.

La vérification avait notamment pour but de déterminer si la CCB avait indûment communiqué à des tiers des renseignements personnels, comme les numéros d'assurance

sociale (NAS) des fermiers. Ces tiers incluaient les manutentionnaires de grains qui facilitent les ventes et l'Agence du revenu du Canada (ARC).

La vérification, effectuée en 2008 et rendue publique en vertu d'une demande d'accès à l'information à l'automne 2009, mettait en lumière de possibles faiblesses sur le plan de la protection de la vie privée. La couverture médiatique subséquente a donné l'impression d'un comportement inapproprié, ce qui a poussé le ministre à déposer une plainte auprès du Commissariat.

Notre enquête a permis de déterminer que la CCB a mis en place les protocoles, les procédures et les accords requis pour veiller à ce que les renseignements personnels des producteurs de grain soient recueillis, utilisés, conservés et communiqués avec soin. Plus précisément, nous avons conclu que la CCB ne communique pas les numéros d'assurance sociale à des tiers et qu'elle transmet des renseignements personnels à l'Agence du revenu seulement lorsqu'elle est tenue de le faire en vertu de la loi.

Par conséquent, il a été conclu que la plainte était ***non fondée***. Nous avons aussi félicité la CCB pour ses bonnes pratiques en matière de gestion de l'information.

4.1.4 UNE PRISON DOIT PLACER LE COURRIER DE NATURE DÉLICATE DANS DES ENVELOPPES APRÈS QU'UN DOCUMENT AIT ÉTÉ INTERCEPTÉ

Un détenu d'un établissement à sécurité maximale près d'Agassiz, en Colombie-Britannique, a déposé une plainte au Commissariat après qu'une décision de dix pages de la Commission nationale des libérations conditionnelles à son sujet ait circulé parmi les autres détenus.

La décision, qui comprenait une description détaillée de l'infraction criminelle du détenu, devait lui être livrée par le biais du courrier interne de l'Établissement de Kent. Plutôt que d'avoir été placé dans une enveloppe, le document a simplement été plié et agrafé, et le nom du détenu a été inscrit à l'extérieur.

La décision de la Commission nationale des libérations conditionnelles n'a jamais été remise au détenu. Il semblerait qu'elle ait été interceptée, photocopiée et diffusée parmi les détenus.

Les responsables de la prison ont écrit au détenu pour l'informer de l'atteinte à la protection des renseignements personnels et de son droit de porter plainte au Commissariat.

Le directeur de l'Établissement de Kent, qui relève du Service correctionnel du Canada, a également lancé une enquête sur l'incident. L'enquête a confirmé que le document

avait été lu par divers détenus sans l'autorisation du plaignant, mais aucune preuve n'a pu démontrer qu'un membre du personnel avait livré le document en question au mauvais détenu de façon intentionnelle.

Notre enquête a révélé que la communication était contraire à la *Loi sur la protection des renseignements personnels* et nous avons conclu que la plainte était ***fondée***.

À la suite de l'incident, le directeur a apporté certains changements au processus de livraison du courrier de l'établissement. Les documents confidentiels sont maintenant placés dans des enveloppes scellées.

4.1.5 UN RAPPORT ÉGARÉ ENTRAÎNE DES CHANGEMENTS DANS UNE PRISON

Deux détenus de l'Établissement Grande Cache du Service correctionnel du Canada, à l'ouest d'Edmonton, ont déposé des plaintes après qu'un rapport de la prison contenant leurs renseignements personnels ait été trouvé parmi les effets personnels d'un autre détenu.

Une enquête menée par l'établissement à sécurité minimale a révélé qu'au début du mois d'avril 2009, un travailleur à forfait avait imprimé une copie d'un rapport, qui contenait le nom, la date de naissance et d'autres renseignements personnels de tous les détenus. Le rapport avait été transmis à un instructeur en soudage, qui l'a emporté dans son bureau dans l'atelier de soudage. Ce dernier le consultait fréquemment lorsqu'il devait interagir avec les détenus.

À la fin du mois de mai 2010, lorsqu'on emballait les effets personnels d'un détenu dans l'aire de mise en liberté de la prison, un agent a découvert le rapport. L'enquête n'a pas réussi à déterminer comment le document s'est retrouvé dans les effets du détenu. Le détenu en question a dit ne pas savoir qu'il avait le rapport et l'instructeur en soudage a nié lui avoir donné.

De plus, l'enquête a révélé que le travailleur à forfait et l'instructeur en soudage avaient reçu une formation sur l'importance de protéger les renseignements personnels.

Les responsables du Service correctionnel ont reconnu l'atteinte à la protection des renseignements personnels de façon officielle. Ils ont également pris certaines mesures pour réduire au minimum le risque de communications inappropriées.

À titre d'exemple, le genre de rapport qui avait été égaré n'est plus imprimé; il ne peut être consulté qu'à l'écran. Des procédures ont aussi été mises en place pour veiller à ce que le personnel et les travailleurs externes comprennent bien à quel point il est important de protéger les renseignements personnels et de s'assurer qu'ils ne sont pas communiqués sans autorisation.

Notre propre enquête a confirmé que le droit à la vie privée des plaignants avait été enfreint et que leurs plaintes étaient ***fondées***. Comme des mesures correctives étaient déjà en voie d'être mises en place, nous n'avons pas recommandé de mesures additionnelles.

4.2 Signalements d'atteintes à la protection des données

4.2.1 APERÇU

Une atteinte à la protection des données est une perte ou une communication non autorisée de renseignements personnels. Certaines atteintes surviennent sans que les personnes touchées ne soient au courant. Dans d'autres cas, les personnes sont avisées de l'atteinte ou l'apprennent d'une autre façon. Certaines de ces personnes déposent une plainte au Commissariat.

Atteintes à la protection des données dans le secteur public fédéral signalées au Commissariat de 2004-2005 à 2010-2011	
2004-2005	27
2005-2006	55
2006-2007	54
2007-2008	44
2008-2009	26
2009-2010	38
2010-2011	64

Peu importe la réaction réelle ou possible des personnes touchées, le gouvernement du Canada a des lignes directrices pour encourager ses ministères et organismes à signaler toute atteinte importante à la protection des données au Commissariat, et ce, de façon opportune.

Au cours du dernier exercice financier, 64 atteintes à la protection des données nous ont été signalées par des institutions fédérales, soit deux tiers de plus que les 38 atteintes qui nous avaient été signalées l'année dernière. Il s'agit du plus grand nombre d'atteintes qui nous ont été signalées au cours des dernières années.

Toutefois, il ne faut pas nécessairement s'alarmer de la hausse des atteintes signalées. Cela pourrait simplement vouloir dire que les organisations sont plus vigilantes pour ce qui est de nous signaler les incidents.

En effet, nous savons qu'un seul ministère, Ressources humaines et Développement des compétences Canada, a signalé 21 incidents l'année dernière, ce qui représente le tiers de tous les signalements que nous avons reçus et trois fois plus que l'année précédente.

Avantages du signalement

Bien que certains ministères se sentent encore mal à l'aise d'admettre leurs erreurs, nous les encourageons tous à nous signaler les atteintes. Lorsqu'ils communiquent avec nous afin d'obtenir des conseils à propos d'un incident, nous leur suggérons toujours de remplir le *Formulaire de rapport d'incident en cas d'atteinte à la vie privée* sur notre site Web et de nous le faire parvenir.

Le Secrétariat du Conseil du Trésor recommande fortement que les institutions avisent le Commissariat de toute atteinte à la protection des données qui :

- touche des données personnelles de nature délicate telles que des renseignements financiers ou médicaux, des numéros d'assurance sociale ou d'autres identificateurs personnels;
- risque d'entraîner un vol d'identité ou une fraude similaire;
- risque de causer un tort ou de l'embarras qui nuirait à la carrière, à la réputation, à la situation financière, à la sécurité, à la santé ou au bien-être d'une personne.

L'institution doit aviser le Commissariat de l'incident et de toutes les mesures d'atténuation prises le plus tôt possible après en avoir pris connaissance, préférablement dans les jours qui suivent.

Les lignes directrices précisent que, dans le cas d'incidents très mineurs, les institutions peuvent décider de régler la situation à l'interne avec les personnes visées, sans en aviser le Commissariat.

De plus, nous savons que la plupart des institutions connaissent maintenant bien leurs obligations en vertu des lignes directrices sur les rapports d'incidents et qu'elles sont prêtes à faire ce qu'il faut. En plus de leur responsabilité de signaler les incidents, elles doivent prendre les mesures nécessaires pour corriger ou atténuer la situation et pour veiller à ce qu'une telle situation ne se reproduise plus.

Il y a aussi des avantages à signaler les incidents.

Par exemple, si nous savons que des mesures de correction sont mises en place, nous pouvons rassurer les personnes qui nous téléphonent pour se plaindre de l'incident en leur disant qu'on s'occupe de cette affaire. Ainsi, ces personnes auront moins tendance à déposer une plainte officielle.

Parmi les 64 atteintes à la protection des données reçues, cinq étaient liées à des renseignements perdus ou volés. Dans deux cas, des employés ont utilisé de façon abusive les renseignements personnels obtenus par le biais de leur emploi en les affichant sur leurs sites Web personnels. Des problèmes techniques étaient à l'origine de quatre de ces atteintes — souvent, une application Web qui n'avait pas été mise à l'essai de façon adéquate.

Dans huit cas, les renseignements personnels d'un tiers n'avaient pas été adéquatement supprimés avant que des documents soient diffusés en réponse à des demandes d'accès à l'information. Dans trois autres cas, des documents contenant des renseignements personnels avaient été laissés dans un bac de recyclage ouvert ou dans un autre endroit accessible au travail.

Pour tous les autres cas, les erreurs ordinaires des employés étaient à la source du problème, par exemple un document contenant des renseignements personnels qui a été envoyé au mauvais destinataire. En effet, année après année, l'erreur humaine relativement à la gestion des données personnelles est la raison la plus courante pour les fuites de données.

RISQUE : ERREUR HUMAINE

Bien qu'il soit impossible d'interdire la distraction, le présent rapport sert toutefois à rappeler, comme chaque année, l'importance de prendre le plus grand soin dans la manipulation des renseignements personnels des Canadiennes et Canadiens. Même en cette ère de distraction, les atteintes à la protection des données causées par l'inattention, la négligence ou autres erreurs humaines devraient pouvoir être évitées.

4.2.2 UN EMPLOYÉ DE TRANSPORT CANADA LAISSE UN CAHIER DANS UN AUTOBUS

Transport Canada nous a informés qu'un de ses employés avait oublié un cahier contenant des renseignements personnels dans un autobus de ville. Le cahier contenait des listes à utiliser en cas d'urgence touchant le système de transport au cours des Jeux olympiques de Vancouver.

Les listes contenaient les numéros d'identification personnels de BlackBerry, ainsi que les numéros de téléphone cellulaire et les numéros de téléphone à la maison d'environ 65 employés fédéraux, jusqu'au niveau de sous-ministre.

Le cahier n'a jamais été retrouvé.

Transport Canada a rappelé à tous ses employés l'importance de bien manipuler les renseignements protégés et classifiés, y compris les procédures qui doivent être suivies lorsque des documents de nature délicate doivent être sortis des locaux du Ministère.

4.2.3 UN EXPERT MÉDICAL OUBLIE DES DOCUMENTS D'EXAMEN DE L'AIDE FINANCIÈRE DANS UN AVION

Un enquêteur médical principal à la tête d'un comité d'examen par les pairs des demandes de financement soumises aux Instituts de recherche en santé du Canada (IRSC) a oublié un ensemble de documents lors d'un vol en direction d'Ottawa. Les documents contenaient des examens de propositions pour des projets universitaires de recherche médicale, afin d'évaluer leur admissibilité à des subventions fédérales.

Il est difficile d'évaluer le nombre exact d'examens qui ont été laissés sur le siège de l'avion, mais on l'estime entre 60 et 70. Ils n'ont jamais été retrouvés.

Une enquête menée par le conseil subventionnaire en recherche médicale a conclu que les documents contenaient des renseignements personnels sur les demandeurs de fonds, mais que l'information n'était pas d'une nature si délicate que le risque de vol d'identité ou autre fraude serait accru.

Dans une lettre envoyée par la suite aux demandeurs de subventions, l'organisation expliquait que, dans la plupart des cas, les documents contenaient des renseignements biographiques que la majorité des chercheurs affichent déjà en ligne.

De plus, l'institution a précisé que, bien que les examens de demande de subventions comprennent généralement l'opinion d'experts externes quant aux compétences de chaque demandeur de subvention, ces documents d'examen étaient plutôt axés sur la composition et l'expertise des équipes de recherche proposées.

Le professeur qui a perdu les documents agissait à titre d'expert externe bénévole dans le processus d'examen des demandes.

Dans la foulée de l'incident, les IRSC ont entrepris de fournir plus d'information sur la sécurité aux examinateurs, y compris sur les pratiques exemplaires en matière de manipulation sécuritaire des documents protégés. L'organisation a également promis d'élaborer une séance d'information sur la sécurité pour les membres bénévoles de ses comités d'examen et de consultation.

4.2.4 DES DOCUMENTS SUR UN PRÊT ÉTUDIANT DESTINÉS À UNE BANQUE ONT ÉTÉ ENVOYÉS À UN AVOCAT PAR ERREUR

Le ministère des Ressources humaines et du Développement des compétences Canada a voulu envoyer une entente de prêt d'études canadien à l'établissement d'enseignement d'une étudiante, mais l'a envoyée à un tiers par erreur.

L'entente et les papiers qui l'accompagnaient contenaient le nom, l'adresse et le numéro de téléphone de l'étudiante, une partie de son numéro d'assurance sociale, son adresse électronique, son programme d'études, son numéro de certificat de prêt, le montant du prêt et son matricule.

Dans ce cas, les documents ont été envoyés à un bureau d'avocats, qui a convenu de les détruire. L'étudiante a été informée de l'incident par lettre.

Un numéro de télécopieur inexact était à la source de l'atteinte à la protection des renseignements personnels. L'entreprise privée responsable des transactions entre le Programme canadien de prêts aux étudiants et les institutions financières a entrepris de vérifier les numéros de télécopieurs des institutions financières au moins une fois par semestre. Elle tiendra aussi un registre pour prendre note de chaque confirmation d'un numéro.

4.2.5 UNE COQUILLE EST À L'ORIGINE D'UNE ERREUR DANS LE COURRIER

Une coquille dans une adresse postale est probablement la raison pour laquelle Travaux publics et Services gouvernementaux Canada a envoyé deux boîtes de documents de nature délicate à une mauvaise adresse à Ottawa.

Les boîtes se sont retrouvées dans le bureau d'un spécialiste des relations gouvernementales. Comme il était habitué de recevoir du matériel imprimé en provenance de ministères fédéraux, son personnel a ouvert les boîtes par erreur.

Quand il a compris que les documents contenaient de l'information personnelle et protégée et qu'ils avaient été envoyés au mauvais endroit, il a communiqué avec le Commissariat. Nous avons ensuite communiqué avec le Ministère.

Une enquête effectuée par l'institution a révélé qu'une série d'erreurs humaines et de la confusion découlant d'un déménagement avaient mené à l'erreur.

L'enquêteur a recommandé un certain nombre de changements aux procédures, y compris de veiller à ce que toutes les enveloppes et les boîtes contiennent l'adresse complète de l'expéditeur. Un formulaire de transmission sécuritaire devrait aussi accompagner toute information protégée et classifiée.

RISQUE : TECHNOLOGIE

Au cours des années précédentes, nous avons été témoins d'atteintes à la sécurité informatique qui avaient exposé des renseignements personnels, parfois de quelques personnes, parfois de dizaines de milliers de personnes. Les pirates informatiques sont quelques fois à blâmer; à d'autres occasions, les failles sont attribuables à des erreurs de programmation ou d'utilisateurs.

Cette année, les problèmes technologiques ont continué de faire des ravages mais, heureusement, peu de personnes ont été touchées.

4.2.6 LE COMPTE EN LIGNE DE SERVICE CANADA RÉVÈLE DES RENSEIGNEMENTS PERSONNELS DE L'UTILISATEUR PRÉCÉDENT

À 11 h 25 le 28 septembre 2010, Ressources humaines et Développement des compétences Canada (RHDCC) a remarqué qu'un problème technique dans le tout nouveau portail en ligne de Service Canada faisait en sorte qu'un utilisateur pouvait voir les renseignements personnels et financiers d'utilisateurs précédents.

À midi, le site Mon dossier Service Canada, lancé le jour précédent, était mis hors service et une enquête interne était lancée.

L'enquête a révélé que le problème provenait d'une composante de l'architecture sous-jacente, appelée Clé d'accès, qui permettait aux gens qui avaient auparavant utilisé une plus vieille technologie (du nom d'epass) de transférer facilement leurs anciens numéros d'identification et mots de passe.

Cette fonction d'ouverture de session automatique a été désactivée et, à 21 h, le site a été réactivé. Il n'y a pas eu d'autre incident.

L'enquête a conclu que, bien que 85 000 personnes avaient utilisé le site lors de sa première journée de fonctionnement, seulement 75 d'entre elles pouvaient avoir été touchées par ce problème technique. Toutes ces personnes ont été contactées et avisées que leurs renseignements personnels avaient peut-être été vus par d'autres.

RHDCC a continué de travailler avec Bell Canada, qui fournit la clé d'accès au nom de Travaux publics et Services gouvernementaux Canada, pour trouver une solution technique permanente et fiable. Les organisations ont aussi entrepris de revoir leurs procédures d'examen afin de réduire les risques qu'un tel problème se répète.

Examen des évaluations des facteurs relatifs à la vie privée

En septembre 2010, nous avons reçu une évaluation des facteurs relatifs à la vie privée de la part de Travaux publics et Services gouvernementaux Canada sur le système d'authentification Clé d'accès.

La Clé d'accès authentifie les personnes et les entreprises dans le cadre de leurs transactions en ligne avec le gouvernement du Canada. Auparavant, les utilisateurs ouvraient une session au moyen d'« epass », une composante de l'infrastructure de la Voie de communication protégée du gouvernement. Ce n'est plus le cas depuis la mise en œuvre du Projet de renouvellement de l'authentification électronique du gouvernement.

Le système d'authentification Clé d'accès est géré par une entreprise privée pour le gouvernement; l'évaluation reçue se servait donc d'une approche interorganisationnelle.

Nos recommandations

Après examen de l'évaluation des facteurs relatifs à la vie privée, nous avons émis une série de recommandations liées à :

- ***la diffusion de lignes directrices sur la collecte, l'utilisation et la communication de données sur les adresses IP;***
- ***l'élaboration de calendriers de conservation et de retrait des renseignements sur les sessions;***
- ***la diffusion d'information plus claire à l'intention des utilisateurs sur la façon dont peuvent être utilisés les renseignements personnels qu'ils fournissent pour obtenir une clé;***
- ***la création de numéros d'identification et de mots de passe sécuritaires pour les utilisateurs.***

4.2.7 UNE AGENCE CINÉMATOGRAPHIQUE AFFICHE DE L'INFORMATION SUR SES CONSULTANTS EN LIGNE

En juillet 2010, Téléfilm Canada, l'agence culturelle fédérale qui développe et fait la promotion de l'industrie audiovisuelle du Canada, a affiché sur son site Web un répertoire de mentors et de consultants en scénarisation, afin d'appuyer le développement professionnel de l'industrie cinématographique en facilitant l'accès à de tels experts bien établis.

Quelques semaines plus tard, un membre de l'unité des services juridiques de Téléfilm a remarqué que le répertoire affichait plus que le nom et les coordonnées des 92 mentors et consultants; plusieurs comprenaient aussi des liens aux curriculum vitae de ces personnes. Les liens ont été immédiatement supprimés.

Téléfilm a lancé une enquête interne, qui a révélé que deux curriculum vitae précisaient le numéro d'assurance sociale et que trois d'entre eux renfermaient les dates de naissance complètes. Téléfilm a informé les cinq personnes touchées de l'atteinte, afin qu'elles puissent prendre les mesures nécessaires pour limiter le risque de vol d'identité ou de mauvaise utilisation de leurs renseignements personnels.

Les curriculum vitae et le répertoire comprenaient également des adresses postales et d'autres renseignements personnels, dont la majorité relevait déjà du domaine public. Téléfilm a conclu que les risques associés à la communication temporaire de ces renseignements étaient minimes.

Par conséquent, l'organisation a décidé de ne pas informer les 87 autres mentors et consultants, question de ne pas les inquiéter indûment.

L'examen interne contenait plusieurs recommandations. L'une d'entre elles consistait à ce que tout document contenant des renseignements personnels soit revu par les avocats de Téléfilm avant d'être affiché sur Internet. L'examen avançait aussi la possibilité de revoir la décision de ne pas informer les mentors et les consultants de l'incident.

4.2.8 DES NUMÉROS D'ASSURANCE SOCIALE APPARAISSENT SUR DES RELEVÉS BANCAIRES

Deux personnes qui recevaient, par dépôt direct, des prestations pour la taxe de vente de l'Ontario gérées par l'Agence du revenu du Canada ont remarqué que leur numéro d'assurance sociale apparaissait sur leurs relevés bancaires.

Elles ont communiqué avec leurs institutions financières, qui ont à leur tour transmis l'information à Travaux publics et Services gouvernementaux Canada (TPSGC).

TPSGC, qui avait effectué le traitement des dépôts au moyen du Système normalisé des paiements, a lancé une enquête.

L'enquête a révélé que le programmeur qui a créé le système pour ces paiements a oublié de chiffrer les numéros d'assurance sociale, dont l'Agence du revenu du Canada se sert à titre de numéro de référence du client.

En tout, le système a effectué 1,8 million de versements par dépôt direct à diverses institutions financières. Ils contenaient tous des numéros d'assurance sociale non chiffrés.

Cependant, en raison d'un caprice propre au système informatique d'une banque, les numéros d'assurance sociale ont été téléchargés et affichés sur les relevés bancaires des prestataires qui étaient des clients de cette banque. Les numéros apparaissaient aussi sur leurs pages bancaires en ligne.

Bien que ce problème technique n'ait pas entraîné plus d'appels au gouvernement ou à la banque, TPSGC l'a corrigé et a pris des mesures pour veiller à ce que tous les versements futurs par dépôt direct comprennent seulement des numéros d'assurance sociale chiffrés.

Le Ministère s'est également engagé à revoir ses procédures de programmation pour les nouveaux produits, de même que ses processus d'assurance de la qualité, et d'offrir de la formation afin d'éviter que la situation se reproduise.

RISQUE : DEMANDES D'ACCÈS À L'INFORMATION

Année après année, il survient des incidents où le traitement de demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* mène à la diffusion involontaire de renseignements personnels qui auraient dû être protégés. Cette année n'a pas été différente des autres.

4.2.9 LA COMMISSION CANADIENNE DES DROITS DE LA PERSONNE DIFFUSE LE NOM D'UN DEMANDEUR D'INFORMATION

La Commission canadienne des droits de la personne a commis ce type d'erreur lorsqu'elle a diffusé par accident le nom d'une personne qui avait fait une demande d'accès à l'information en vertu de la *Loi*.

Le nom de la personne, qui aurait dû demeurer confidentiel, a été inclus dans une lettre à un tiers, que l'on consultait pour savoir si une partie ou l'ensemble de l'information devait être diffusée.

La Commission a avisé le tiers qu'il avait reçu le nom du demandeur par erreur et a demandé qu'il protège le nom et ne le diffuse pas. Le demandeur en question a également été avisé de l'incident.

4.3 Système national intégré d'information interorganismes et Outil de recherche intégré — évaluations des facteurs relatifs à la vie privée de la GRC

En 2010-2011, nous avons continué à revoir les évaluations des facteurs relatifs à la vie privée liées à un grand projet en évolution constante permettant à la Gendarmerie royale du Canada (GRC) et aux forces policières provinciales, territoriales, autochtones et municipales d'échanger des données d'enquête qu'elles recueillent entre elles et avec des ministères fédéraux.

La structure de partage de données du Système national intégré d'information interorganismes (N-III) comporte deux systèmes.

- Le premier est le Portail d'informations policières (PIP), qui permet aux organismes de police de partager des renseignements détaillés concernant les incidents, provenant de leurs systèmes de gestion des dossiers respectifs. Il existe de nombreux systèmes de gestion des dossiers au sein des corps policiers à l'échelle du Canada. Un de ces systèmes est le SIRP de la GRC, le Système d'incidents et de rapports de police, décrit à la section 2.2 de ce rapport.

- Le deuxième élément de la structure de partage de données du N-III est l'Outil de recherche intégré, qui est utilisé par les ministères et les organismes fédéraux œuvrant dans le domaine de la sûreté et de la sécurité du public pour accéder aux renseignements de police contenus dans le PIP. En tout, 34 institutions fédérales ont accès au PIP. Certaines d'entre elles, comme l'Agence des services frontaliers du Canada, Passeport Canada et le Centre d'analyse des opérations et déclarations financières du Canada, ont utilisé l'Outil de recherche intégré.

Nous avons reçu et revu une évaluation globale des facteurs relatifs à la vie privée pour ce programme de la part de Sécurité publique Canada, de même que plusieurs évaluations connexes en provenance d'organismes fédéraux participants.

Nos inquiétudes

À la suite de nos examens, nous continuons à être inquiets de la portée du partage des renseignements sur les incidents et les dossiers de cas.

Contrairement à la base de données du Centre d'information de la police canadienne (CIPC), qui contient des renseignements factuels à propos des accusations criminelles et de leur cheminement au sein du système judiciaire (voir la section 2.2 pour plus de renseignements), le PIP permet d'accéder à des systèmes de dossiers criminels contenant de l'information détaillée à propos des témoins, des victimes, des membres de la famille et d'autres personnes liées à une enquête, même de façon indirecte, ou de l'information fournie par ces personnes.

De tels renseignements peuvent être très subjectifs et pourraient, en fait, ne pas être liés à des actes répréhensibles. S'ils sont utilisés sans contexte ou mesures de protection appropriées, ils pourraient entraîner de fâcheuses conséquences pour d'innocentes personnes.

Nos recommandations

Nous continuons à promouvoir la mise en place de mesures de contrôle publiques transparentes pour ce qui est du partage de cette information. La responsabilité de la gestion de cette information doit relever de Sécurité publique Canada.

Parmi nos autres recommandations, nous avons demandé à Sécurité publique Canada de nommer un responsable de la protection de la vie privée pour surveiller l'utilisation des renseignements personnels contenus dans le PIP.

4.4 Suivis de vérifications antérieures

En vertu de l'article 37 de la *Loi sur la protection des renseignements personnels*, la commissaire à la protection de la vie privée peut, à sa discrétion, mener des vérifications pour veiller à ce que les ministères et les organismes fédéraux respectent les articles 4 à 8 de la *Loi*. Ces articles concernent la collecte, l'utilisation, la conservation, la communication et le retrait des renseignements personnels qui se trouvent entre les mains des organisations.

Si une vérification révèle des lacunes relativement à la conformité, la commissaire peut recommander des mesures de correction. Ces recommandations sont faites à l'institution et peuvent être publiées dans des rapports annuels ou spéciaux au Parlement.

Comme la *Loi* ne lui procure pas d'autres pouvoirs d'application, le Commissariat mène parfois des vérifications de suivi pour déterminer si une organisation qui a déjà été vérifiée suit nos recommandations ou donne suite aux engagements pris dans le passé.

Cette année, nous avons effectué un suivi sur trois vérifications antérieures. Une de ces vérifications, qui portait sur l'utilisation des fichiers inconsultables de la GRC, est décrite à la section 2.5 du présent rapport. Deux autres vérifications, où un élément clé était la protection des renseignements personnels contre une communication inappropriée, sont décrites ci-dessous :

- Opérations liées au passeport canadien (2008)
- Cadres de gestion de la protection de la vie privée de certaines institutions fédérales (2009)

De façon globale, nous avons conclu que les institutions vérifiées avaient répondu de façon positive : 32 des 34 recommandations que nous avions faites dans les trois vérifications de suivi — 94 % — avaient été entièrement ou presque complètement mises en œuvre, et des mesures avaient été entreprises sur une autre.

4.4.1 OPÉRATIONS LIÉES AU PASSEPORT CANADIEN

Nous avons vérifié les progrès accomplis par Passeport Canada, un organisme de service spécial du ministère des Affaires étrangères et du Commerce international (MAECI), depuis la clôture de notre vérification de ses activités en décembre 2008. La vérification soulignait certaines lacunes qui posaient un risque important à la protection des renseignements personnels des demandeurs de passeport.

Plus précisément, nous avons remarqué des faiblesses liées au processus de demande, à la façon dont les renseignements personnels sont recueillis et conservés, à la façon d'y accéder et à la façon dont ils sont éliminés.

Nous avons fait 15 recommandations visant l'amélioration des mesures de protection des renseignements personnels de l'organisme.

Réponse de Passeport Canada et du MAECI

Jusqu'à maintenant, Passeport Canada et son ministère d'attache nous ont signalé qu'ils ont entièrement, ou de façon très importante, mis en œuvre 14 de ces recommandations et que celle qui reste a été abordée en partie.

Les deux institutions nous ont entre autres expliqué qu'elles avaient entrepris les activités suivantes en réponse à notre vérification :

- ***mise en place de procédés et de mesures de protection techniques afin de réduire au minimum le risque d'accès inapproprié aux renseignements liés aux passeports;***
- ***modification de la configuration des cloisons de service au public de Passeport Canada pour rehausser la protection des renseignements personnels des clients;***
- ***baisse du délai de conservation des demandes de passeport et de la documentation connexe;***
- ***cryptage des liens de réseau entre Passeport Canada et le ministère des Affaires étrangères et du Commerce international, de même que des données conservées dans le Système de gestion des cas de Passeport Canada;***
- ***établissement d'une directive sur les atteintes à la protection des renseignements personnels.***

Bien qu'il reste du travail à accomplir pour pleinement donner suite à toutes nos recommandations, nos activités de suivi indiquent que des progrès importants ont été faits afin de renforcer les mesures de contrôle visant à protéger les renseignements personnels des demandeurs de passeport.

4.4.2 CADRES DE GESTION DE LA PROTECTION DE LA VIE PRIVÉE DE CERTAINES INSTITUTIONS FÉDÉRALES

En février 2009, la commissaire a soumis un rapport spécial au Parlement, décrivant notre examen des cadres de gestion de la protection de la vie privée de quatre institutions fédérales — Élections Canada, Passeport Canada, l'Agence du revenu du Canada et le groupe Service Canada du ministère qui était connu à l'époque sous le nom de Ressources humaines et Développement social Canada.

Le cadre de gestion de la protection de la vie privée de chaque institution se trouvait à différentes étapes de maturité. Nous avons noté de bonnes pratiques en matière de protection des renseignements personnels, mais aussi des possibilités d'amélioration.

Nous avons formulé 15 recommandations dont un bon nombre portait sur le renforcement de la gouvernance et de la reddition de comptes en matière de protection des renseignements personnels, sur le besoin d'offrir plus de séances de sensibilisation sur cette question et sur la correction de lacunes dans la gestion des ententes d'échange de renseignements.

Réponses des institutions

Les institutions vérifiées nous ont toutes indiqué qu'elles avaient entièrement, ou de façon importante, mis en place 14 de nos 15 recommandations. À titre d'exemple :

- ***Élections Canada a supprimé de sa base de données tous les renseignements sur les personnes âgées de moins de 18 ans et a mis en place des mesures pour veiller à ce que les risques pour la protection de la vie privée soient pris en compte dans le cadre de nouvelles initiatives.***
- ***Le ministère maintenant appelé Ressources humaines et Développement des compétences Canada a renforcé et regroupé ses processus de gouvernance et de surveillance en matière de protection des renseignements personnels. Il a aussi créé un inventaire ministériel des ententes d'échange de renseignements personnels.***
- ***L'Agence du revenu du Canada a élaboré un ensemble de politiques en matière de protection de la vie privée qui officialisent et définissent les rôles, les responsabilités et la reddition de comptes au sein de l'institution. De plus, la Direction de la sécurité et des affaires internes et la Direction de l'accès à l'information et de la protection des renseignements personnels ont mis en place une entente d'échange de renseignements pour le signalement des atteintes à la protection des renseignements personnels.***

Nous continuerons à surveiller les progrès accomplis par ces institutions relativement à la mise en œuvre complète des recommandations de la commissaire.

4.5 Communications en vertu de l'alinéa 8(2)*m*) de la *Loi sur la protection des renseignements personnels*

L'alinéa 8(2)*m*) de la *Loi sur la protection des renseignements personnels* permet à une institution de communiquer des renseignements personnels sans le consentement de l'individu concerné si, de l'avis du responsable de l'institution :

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

Les institutions qui prévoient communiquer des renseignements pour des raisons d'intérêt public doivent en aviser le Commissariat par écrit — avant que cette communication n'ait lieu, si les circonstances le permettent; sinon, elles doivent le faire tout de suite après.

Le Commissariat examine la communication, et si la personne dont les renseignements personnels seront communiqués n'a pas été avisée et que nous croyons qu'elle doit l'être, nous encouragerons le ministère à l'aviser. En général, les ministères suivent nos conseils, mais s'ils refusent, la commissaire a l'autorité d'aviser elle-même la personne.

Au cours de l'exercice financier 2010-2011, nous avons traité 80 communications en vertu de l'alinéa 8(2)*m*), une baisse de près d'un quart comparativement aux 104 communications traitées l'année précédente.

Communications les plus courantes

- *Ministère des Affaires étrangères et du Commerce international*

Le ministère des Affaires étrangères et du Commerce international a effectué 34 communications en 2010-2011, soit le plus grand nombre parmi toutes les institutions. Généralement, le Ministère communique aux autorités de santé publique provinciales et territoriales les coordonnées de gens qui pourraient avoir été exposés à la tuberculose infectieuse par un autre passager sur un vol.

Dans un autre cas, le Ministère a communiqué l'information contenue dans la demande de passeport d'une femme décédée à ses deux fils, afin de leur permettre de confirmer qu'elle était née au Canada et de faire une demande de citoyenneté canadienne.

- *Service correctionnel du Canada*

Le Service correctionnel du Canada a effectué 16 communications en vertu de l'alinéa 8(2)*m*), généralement pour deux raisons : informer les médias ou les groupes de services aux victimes qu'un détenu s'est échappé ou que des incidents violents ont eu lieu dans un établissement et informer les membres d'une famille des circonstances dans lesquelles un détenu est décédé.

En outre, le service a communiqué en juin et septembre 2010 les renseignements personnels d'une détenue décédée à l'Association canadienne des sociétés Elizabeth Fry à la suite d'une décision rendue par la Cour fédérale.

- *Gendarmerie royale du Canada*

La Gendarmerie royale du Canada (GRC) a effectué 10 communications d'intérêt public au cours du dernier exercice financier. Certaines étaient liées à des personnes qui devaient être libérées dans la communauté après avoir purgé une peine pour agression sexuelle ou pour possession de pornographie juvénile. Il y a aussi eu des cas où de l'information sur des infractions sexuelles a été divulguée à des postes de police locaux pour une enquête plus approfondie.

Autres exemples

D'autres communications ont été faites en vertu de l'alinéa 8(2)*m*) l'année dernière dans les cas suivants :

- La Commission de l'immigration et du statut de réfugié a indiqué sur son site Web qu'elle avait interdit à une personne de comparaître devant la Commission à titre de conseil tant qu'elle ne serait pas convaincue qu'elle ne facture pas de frais pour ses services. L'information a aussi été communiquée à la Société canadienne de consultants en immigration, ainsi qu'à tous les barreaux provinciaux et territoriaux.

- En décembre 2010, le Bureau du vérificateur général a déposé un rapport de vérification qui comprenait des renseignements personnels au sujet de l'ancienne commissaire à l'intégrité du secteur public du Canada.

CHAPITRE 5

Le CPVP à l'œuvre

Renforcer le droit des Canadiennes et des Canadiens à la vie privée

À la suite de sa reconduction pour un deuxième mandat en décembre 2010, la commissaire à la protection de la vie privée, Jennifer Stoddart, a mis en évidence les trois priorités suivantes pour les trois prochaines années :

- exercer un leadership pour promouvoir les domaines prioritaires en matière de protection de la vie privée;
- aider les Canadiennes et Canadiens, les organisations et les institutions à prendre des décisions plus éclairées en matière de protection de la vie privée;
- offrir des services au Parlement et à l'ensemble de la population canadienne.

Bien entendu, notre travail en ce sens a débuté il y a bon nombre d'années et, comme le décrivent les chapitres précédents de ce rapport annuel, nous avons fait des progrès notables au cours de 2010-2011.

Ce chapitre souligne le travail additionnel que nous avons fait pour faire progresser notre mission, qui consiste à protéger et à promouvoir le droit des individus à la vie privée.

Le présent chapitre explique comment nous répondons aux demandes de renseignements et aux plaintes de citoyens qui croient que les ministères et les organismes ont enfreint leurs droits. Il décrit aussi notre travail en appui au Parlement et aux institutions fédérales, de même que nos efforts pour accroître le niveau de connaissances liées aux questions de protection de la vie privée.

Dans ce chapitre, vous trouverez les sections suivantes :

5.1 Notre travail de « première ligne »

5.1.1 DEMANDES DE RENSEIGNEMENTS

***Reçues* :** En 2010-2011, nous avons reçu 1 944 demandes de renseignements de la part des Canadiennes et Canadiens sur des questions de protection de la vie privée découlant de leurs interactions avec le gouvernement du Canada. Nous avons reçu 2 188 demandes de renseignements additionnelles sur des questions liées à la protection de la vie privée, mais il était difficile de déterminer si c'était la loi sur la protection des renseignements personnels visant le secteur public ou celle visant le secteur privé qui s'appliquait.

Le nombre de demandes de renseignements a baissé de 24 % comparativement à l'année dernière. Comme les visites sur le site Web du Commissariat continuent de grimper — une hausse de 31 % depuis 2007-2008 pour un total de 2,2 millions de visiteurs en 2010-2011 —, nous supposons que plus de gens vont en ligne pour obtenir des réponses à leurs questions. Par ailleurs, nous avons enregistré 1,01 million de visites sur nos blogues et autres sites Web au cours du dernier exercice financier, un nombre semblable à celui de l'exercice précédent.

Réglées : La Section des demandes de renseignements a répondu à 1 859 demandes liées directement à la *Loi sur la protection des renseignements personnels* en 2010-2011, soit 30 % de moins que l'année précédente. La plupart de ces demandes (56 %) ont été effectuées par téléphone. Certaines personnes nous ont également transmis leurs demandes par la poste, par télécopieur ou par courriel, et d'autres se sont présentées au Commissariat.

Nous avons reçu 2 183 demandes de renseignements additionnelles pour lesquelles il était impossible de déterminer à quelle loi elles étaient liées ou auxquelles ni l'une ni l'autre des lois en matière de protection des renseignements personnels ne pouvaient s'appliquer — une baisse de 24 % comparativement à 2009-2010. (Voir l'annexe 3 pour l'ensemble des statistiques.)

5.1.2 PLAINTES RÉGLÉES RAPIDEMENT

Afin de continuer à offrir un service amélioré aux Canadiennes et Canadiens, nous savons qu'il faut traiter leurs questions et leurs inquiétudes de façon efficace et efficiente. Le règlement rapide des plaintes joue un rôle important à cet égard. La meilleure façon d'accélérer le processus est de conclure la plainte de façon satisfaisante sans ouvrir d'enquête officielle.

Nous avons donc accru nos efforts pour résoudre les plaintes sans enquêtes et nous avons affecté un agent à cette tâche.

Il est souvent possible de régler rapidement une plainte en partageant de l'information avec le plaignant ou le ministère et en dissipant les malentendus.

Par exemple, les plaignants sont parfois satisfaits si on leur dit comment des plaintes semblables ont été réglées dans le passé. S'il a été déterminé par le passé que les ministères, dans des circonstances similaires, avaient respecté la *Loi sur la protection des renseignements personnels*, les plaignants ont tendance à accepter qu'il ne sert à rien de procéder à une autre enquête.

De même, les plaignants qui ont demandé, en vain, d'avoir accès à leurs renseignements personnels pourraient ne pas connaître les exceptions prévues par la *Loi* que les ministères ont le droit d'appliquer. Lorsqu'ils comprennent la loi, certains plaignants sont satisfaits et l'affaire est considérée comme réglée.

Règlement rapide

Lorsqu'une plainte est déposée en vertu de la *Loi sur la protection des renseignements personnels*, le registraire des plaintes détermine si elle pourrait être réglée rapidement, en fonction de facteurs comme la complexité apparente du cas, et si elle touche à des questions qui ont été traitées dans le passé.

Dans environ un quart des cas, la question ne peut être réglée rapidement ou les parties n'arrivent pas à s'entendre. Dans ces situations, le cas est réaffecté pour enquête officielle.

En moyenne, il nous a fallu 3,6 mois pour fermer nos dossiers de règlement rapide en 2010-2011, comparativement à huit mois pour les dossiers qui nécessitent des enquêtes officielles.

De nombreux facteurs contribuent au règlement relativement rapide des dossiers qui ne nécessitent pas une enquête officielle. Parfois, par exemple, la question peut être réglée avec un simple coup de fil.

De plus, tandis que les enquêtes se terminent par la rédaction d'une lettre de conclusions d'enquête officielle, ce qui peut prendre du temps, les cas de règlement rapide sont résumés dans des rapports internes qui servent de documents de référence pour les cas semblables à l'avenir.

En 2010-2011, nous avons reçu 98 plaintes que nous avons jugées susceptibles d'être réglées de façon rapide. De ce nombre, 15 plaintes ont été reçues plus tard au cours de l'exercice financier et étaient toujours non réglées en date au 31 mars 2011.

Des 83 plaintes reçues et réglées au cours de l'exercice financier, 61 ont été réglées rapidement, et 22 ont été affectées à des enquêteurs, pour diverses raisons.

De plus, nous avons réussi à traiter, au cours de 2010-2011, 17 des 22 dossiers de règlement rapide qui avaient été ouverts en 2009-2010. Les cinq autres dossiers reportés ont été transmis à des enquêteurs.

Signé, scellé et livré

Un homme s'est plaint de ce qu'il a perçu comme étant une infraction à la *Loi sur la protection des renseignements personnels* par Postes Canada après qu'on lui ait demandé de fournir une signature lue optiquement lorsqu'il a ramassé un colis.

Notre agent de règlement rapide a communiqué avec Postes Canada, qui a indiqué que les personnes ne sont pas obligées de signer pour un colis. Elles peuvent inscrire leur nom en caractères d'imprimerie, leurs initiales ou alors simplement refuser de signer. Si une signature électronique est fournie, l'expéditeur du colis peut se servir d'un numéro d'identification personnel désigné pour la voir sur le site Web de l'organisme pour une période de 60 jours.

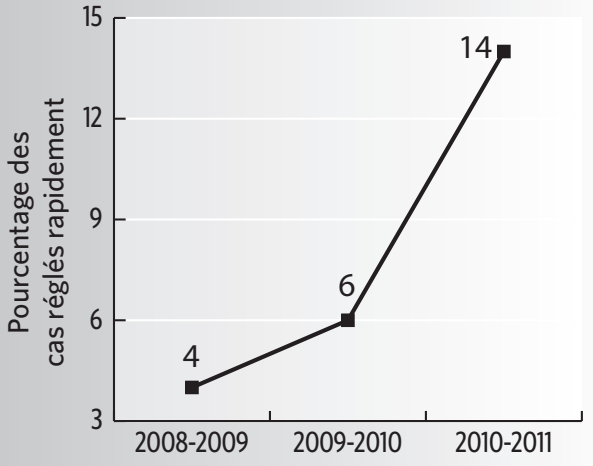
Nous avons transmis ces renseignements au plaignant, qui a dit être content de savoir qu'il n'avait pas besoin de fournir une signature. La question a été considérée résolue.

En 2010-2011, 78 plaintes qui, dans le passé, auraient probablement été traitées au moyen d'enquêtes exigeant beaucoup de ressources ont été réglées rapidement et de façon satisfaisante par le biais du processus de règlement rapide. Sur les 105 dossiers qui avaient été ciblés comme pouvant être réglés de façon rapide, cela représente un taux de réussite de 74 %.

PROGRÈS GRADUELS

Les 78 dossiers mentionnés ci-dessus représentent 14 % de tous les dossiers que nous avons fermés au cours de l'exercice financier.

PROPORTION DE DOSSIERS FERMÉS AU MOYEN DE STRATÉGIES DE RÈGLEMENT RAPIDE (%)



En comparaison, 68 dossiers ont été fermés en 2009-2010 au moyen de stratégies de règlement rapide, ce qui ne représentait que 6 % du nombre de cas de l'année. L'année précédente, nous avions fermé 42 des 990 dossiers (4 %) de cette façon.

Bien que cette tendance soit réconfortante, en réalité, les progrès sont lents. Le règlement rapide n'est pas toujours l'option appropriée pour traiter les plaintes.

Certaines questions, par exemple, sont trop complexes. D'autres révèlent des problèmes systémiques. D'autres encore semblent, à première vue, constituer une atteinte si grave à la protection de la vie privée qu'une enquête est requise. De tels cas sont transmis directement à un enquêteur.

Bien que nous n'ayons pas eu l'occasion d'examiner la question de façon officielle, nous avons remarqué plusieurs autres facteurs qui nous empêchent d'appliquer pleinement l'approche de règlement rapide.

À titre d'exemple, certains plaignants produisent des dossiers contenant des douzaines et même des centaines de demandes d'accès aux renseignements personnels, conservés dans des bases de données de nombreuses institutions fédérales. Dans de tels cas, le règlement rapide est peu probable.

De plus, il est plus difficile de « satisfaire les clients » dans le secteur public qu'il ne l'est dans le secteur privé. En effet, une banque peut dispenser un client de certains frais afin de le satisfaire ou un magasin peut offrir un produit gratuit à titre de réparation. Le gouvernement a moins d'options pour résoudre les différends de façon rapide et relativement officieuse.

Nous faisons tout de même preuve d'un optimisme prudent pour ce qui est des résultats de nos efforts en matière de règlement rapide jusqu'à maintenant. Le taux de réussite a augmenté, même si ce n'est que de façon modeste, et nous continuerons d'apprendre de nos expériences et d'en tirer profit. Nous avons l'intention de poursuivre nos efforts dans ce sens au cours des années à venir.

5.1.3 PLAINTES

En tout, nous avons reçu 708 plaintes l'année dernière, soit une hausse de 6 % par rapport aux 665 de l'exercice 2009-2010. Même si nous avons réussi à traiter 76 d'entre elles grâce à des stratégies de règlement rapide, 632 dossiers ont été envoyés à nos enquêteurs en 2010-2011.

Par le passé, la raison la plus courante pour le dépôt de plaintes au Commissariat était la perception qu'une institution fédérale prenait trop de temps pour répondre aux demandes de renseignements personnels.

Toutefois, en 2010-2011, les plaintes liées aux délais* sont arrivées en deuxième place, représentant 251 des 708 plaintes reçues (36 %). Les plaintes les plus courantes portaient sur les problèmes liés à l'accès aux renseignements personnels. Nous avons reçu 328 plaintes de ce type, soit 46 % de l'ensemble des plaintes.

Les autres plaintes (129 ou 18 %) étaient liées à la collecte, à l'utilisation, à la communication ou à la conservation des renseignements personnels par les ministères ou les organismes gouvernementaux†.

Types de plaintes le plus souvent reçues

	Nombre	Pourcentage
Accès : Difficultés éprouvées relativement à l'accès aux renseignements personnels	328	46
Délais : Inquiétudes quant au temps de réponse d'une institution à une demande d'accès aux renseignements personnels.	251	36
Protection des renseignements personnels : Inquiétudes relatives à la collecte, à l'utilisation, à la communication, à la conservation ou au retrait de renseignements personnels par une institution.	129	18
Total	**708**	**100**

En 2010-2011, la majorité des plaintes provenaient de l'Ontario (30 %), du Québec (27 %) et de la Colombie-Britannique (23 %). Une tendance semblable est observée plus ou moins chaque année et reflète la répartition de la population du Canada.

Les Canadiennes et Canadiens qui habitent à l'étranger ont le même droit d'accès à leurs renseignements personnels que ceux qui habitent au Canada. Deux personnes ont exercé ce droit en 2010-2011.

Comme par les années passées, la plupart des plaintes reçues (276, soit 39 % du total) étaient dirigées contre le Service correctionnel du Canada. Toutes les plaintes, à l'exception de 23 d'entre elles, provenaient de gens qui avaient de la difficulté à accéder

* Les types de plaintes sont définis à l'annexe 1.

† Les tableaux de données détaillés se trouvent à l'annexe 3.

à leurs renseignements personnels ou qui trouvaient que l'institution avait pris trop de temps pour répondre à leurs demandes d'accès à l'information.

Le nombre de plaintes déposées contre ce ministère en 2010-2011 était en baisse de 5 % comparativement aux 290 plaintes déposées l'année précédente. Cependant, la tendance générale est à la hausse : une augmentation de 42 % du nombre de plaintes déposées contre le Service correctionnel du Canada a été observée depuis 2006-2007.

Comme pour les années précédentes, la Gendarmerie royale du Canada (GRC), le ministère de la Défense nationale et l'Agence du revenu du Canada suivaient avec 75, 65 et 53 plaintes respectivement.

Les ministères qui ont fait l'objet de nombreuses plaintes cette année font généralement partie de notre liste des 10 institutions contre lesquelles le plus de plaintes avaient été déposées dans les années précédentes. En raison de leurs mandats, certaines institutions doivent conserver une grande quantité de renseignements personnels. Par conséquent, il est plus probable qu'elles reçoivent de nombreuses demandes d'accès à ces renseignements, ce qui peut ainsi mener à des plaintes sur la façon dont ces renseignements sont manipulés.

Le nombre de plaintes déposées contre une institution ne veut pas nécessairement dire qu'elle ne se conforme pas à la *Loi sur la protection des renseignements personnels*; cette détermination ne peut être faite qu'au moyen d'une enquête.

En 2010-2011, Anciens Combattants Canada a joint les rangs des 10 institutions contre lesquelles le plus grand nombre de plaintes ont été déposées. L'institution a reçu 15 plaintes, comparativement à seulement deux l'année précédente. Une de ces plaintes a fait l'objet d'une enquête exhaustive, dont le résultat a mené à la tenue d'une vérification de la conformité à la protection de la vie privée. Voir la section 3.1 du présent rapport pour de plus amples renseignements.

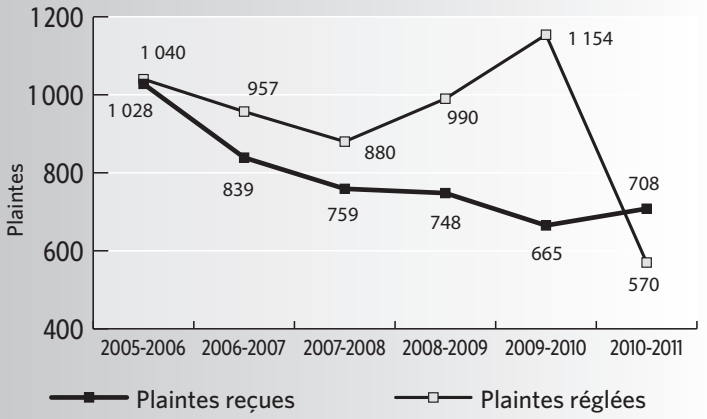
5.1.4 Enquêtes et autres décisions

Nous avons pu fermer un total de 570 dossiers de plaintes en 2010-2011, soit presque la moitié des 1 154 dossiers que nous avons fermés l'année précédente. Cette baisse s'explique essentiellement par le fait que des ressources additionnelles avaient été accordées pour une période de deux ans se terminant à la fin de 2009-2010. Ces fonds avaient été versés précisément pour éliminer l'arriéré d'enquêtes. Au début de 2008-2009, cet arriéré comptait 575 plaintes reçues depuis plus d'un an.

Grâce à ces fonds, nous avions embauché des enquêteurs et élaboré un ensemble de stratégies qui nous ont permis de diminuer notre arriéré de dossiers à seulement 10 à la fin de 2009-2010.

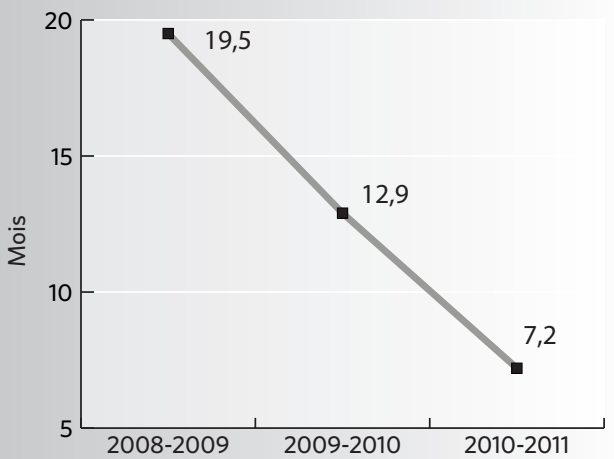
Toutefois, sans ces ressources humaines et financières additionnelles, nous n'avons pu continuer à traiter le même nombre de plaintes que l'année dernière. À la fin de 2010-2011, notre arriéré contenait 35 dossiers.

APERÇU SUR SIX ANS DES PLAINTES REÇUES ET RÉGLÉES



En revanche, l'accent que nous mettons sur le règlement rapide des plaintes nous permet de réduire le temps de règlement de chaque dossier, d'une moyenne pondérée de 19,5 mois en 2008-2009 à 12,9 mois en 2009-2010 et à seulement 7,2 mois en 2010-2011. Cela représente une baisse de 63 % du délai de traitement en seulement deux ans.

TEMPS REQUIS POUR RÉGLER LES PLAINTES



En effet, le délai de traitement moyen des 78 cas de règlement rapide que nous avons fermés en 2010-2011 était de

seulement 3,6 mois — moins de la moitié des huit mois qu'il nous a fallu pour régler un cas moyen par l'entremise d'une enquête.

Cela nous laisse à penser que si nous continuons à accroître la proportion de plaintes qui peuvent être réglées sans enquêtes officielles, nous pouvons diminuer davantage le temps moyen qu'il nous faut pour traiter l'ensemble des plaintes.

DÉCISIONS

Type de plainte		Conclusions d'enquête			Autres issues			Total
		Fondée*	Non fondée	Résolue	Abandonnée	Réglée rapidement	Réglée en cours d'enquête	
Accès	Accès	32	108	13	20	26	6	**205**
	Correction/ annotation	1	0	0	0	3	0	**4**
	Frais	0	0	0	0	1	0	**1**
	Langue	2	0	0	0	0	0	**2**
Délais	Avis de prorogation	12	10	0	2	0	0	**24**
	Délais	208	13	0	6	6	0	**233**
Protection des renseignements personnels	Collecte	1	4	0	0	9	0	**14**
	Conservation et retrait	4	1	0	3	0	0	**8**
	Utilisation et communication	21	13	0	10	33	2	**79**
Total		**281**	**149**	**13**	**41**	**78**	**8**	**570**

À part les 78 cas traités au moyen du processus de règlement rapide, 492 des 570 dossiers fermés en 2010-2011 ont été affectés à des enquêteurs. De ce nombre, 41 cas ont été abandonnés par le plaignant. Huit autres cas ont été réglés en cours

* Comprend 31 cas d'accès auparavant classés comme « fondés et résolus ».

d'enquête. Par conséquent, 443 cas ont été réglés au moyen d'une enquête au terme de laquelle nous avons émis des conclusions officielles.

Fondées : Dans 281 cas (63 %), nous avons été en accord avec le plaignant. Le plus souvent, nous avons validé une plainte lorsque l'organisation mise en cause n'avait pas permis au plaignant d'accéder à ses renseignements personnels de façon opportune. Dans 220 cas (79 %), nous avons conclu que les plaintes déposées en raison des délais étaient « fondées ».

Ce constat n'est pas surprenant et est en fait conforme à nos observations des années précédentes. De façon générale, les plaignants déposent une plainte seulement après que la période de 30 jours, durant laquelle les organisations sont habituellement censées fournir les renseignements personnels, se soit écoulée. Si le délai réglementaire est écoulé et que l'institution n'a pas d'argument convaincant pour le proroger, la plainte est alors fondée, presque par définition.

Non fondée : Dans 149 cas, soit un peu plus du tiers de nos 443 enquêtes, nous avons conclu que la plainte n'était pas fondée.

Dans 108 de ces cas non fondés (72 %), la plainte découlait d'une demande infructueuse d'accès aux renseignements personnels. La *Loi sur la protection des renseignements personnels* comprend plusieurs exceptions ou raisons pour lesquelles les ministères et les organismes peuvent refuser de communiquer les renseignements personnels qu'ils ont en leur possession. Si l'enquête menée sur une plainte d'accès révèle qu'une exception a été invoquée ou appliquée de façon adéquate, nous concluons alors habituellement que la plainte n'est pas fondée.

Résolue : Treize autres cas, portant sur des plaintes liées à l'accès aux renseignements personnels, ont été résolus après qu'une enquête approfondie ait liée le problème à un malentendu. Dans ces cas, nous avons conclu que l'allégation était justifiée, mais qu'une entente négociée était possible.

Plaintes concernant la protection des renseignements personnels : La catégorie des plaintes liées à la protection des renseignements personnels concerne la collecte, l'utilisation, la communication, la conservation et le retrait des renseignements personnels. En tout, nous avons enquêté sur 101 plaintes de ce genre en 2010-2011, soit environ 18 % des 570 cas que nous avons fermés.

Plus de la moitié de ces cas ont été abandonnés (13), réglés rapidement (42) ou réglés en cours d'enquête (2).

Sur les 44 cas liés à la protection des renseignements personnels et dans le cadre desquels une enquête complète à été menée, nous avons conclu que 26 étaient fondés et 18 non fondés. Sans égard aux conclusions, la majorité des enquêtes sur la protection des renseignements personnels que nous avons menées à terme portaient sur l'utilisation ou la communication inappropriée de renseignements personnels.

Des statistiques détaillées sur la conclusion de toutes les plaintes se trouvent à l'annexe 3.

5.2 Appui au Parlement

5.2.1 COMPARUTIONS DEVANT LE PARLEMENT

Au cours de 2010-2011, la commissaire, la commissaire adjointe et d'autres représentants du Commissariat ont témoigné 15 fois de façon officielle devant les députés et les sénateurs, dont 14 fois pour parler de sujets touchant en bonne partie le secteur public. Parmi les sujets abordés :

- les répercussions des mesures liées à la sûreté aérienne sur la protection de la vie privée;
- la prolongation du mandat de sept ans de la commissaire pour trois autres années;
- les nouvelles initiatives législatives comme la *Loi canadienne sur la sécurité des produits de consommation* et la *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*;
- les modifications apportées au *Code criminel* pour protéger les victimes des délinquants sexuels;
- la décision de rendre le formulaire long du recensement de 2011 facultatif plutôt qu'obligatoire.

5.2.2 SÛRETÉ AÉRIENNE

En 2010-2011, nous avons continué à exprimer nos inquiétudes à propos des répercussions de certaines mesures législatives liées à la sûreté aérienne sur la protection de la vie privée, y compris le Système d'information préalable sur les voyageurs/Dossier

passager, le Programme de protection des passagers et le programme Secure Flight en vertu de ce qui était auparavant appelé le projet de loi C-42.

Ces mesures ont entraîné la création d'immenses bases de données gouvernementales, l'utilisation de listes secrètes d'interdiction de vol, la surveillance plus étroite des voyageurs et des employés d'aéroport et le partage accru d'information avec les gouvernements étrangers.

Par exemple, le projet Secure Flight, contenu dans le projet de loi C-42, permet notamment aux autorités américaines de recueillir des renseignements personnels sur les voyageurs à destination et en provenance du Canada qui survolent l'espace aérien américain. Cette mesure permet ainsi aux autorités américaines d'interdire à certaines personnes de se rendre au Canada ou d'en revenir.

Lors de notre témoignage devant le comité parlementaire sur cette initiative, nous avons affirmé que le gouvernement du Canada a le devoir de protéger les droits civils et le droit à la vie privée de ses citoyens.

Nous reconnaissons que la sûreté aérienne a toujours été importante et, pour des raisons que nous comprenons tous, elle est devenue une priorité au Canada et partout dans le monde. Néanmoins, nous sommes d'avis que la sécurité et la protection de la vie privée peuvent cohabiter; ces deux éléments ne sont pas incompatibles.

D'un point de vue pratique, la protection de la vie privée nécessite que la collecte de renseignements personnels soit minimale, que les périodes de conservation soient limitées, que les Canadiennes et Canadiens soient informés de la portée de la collecte de renseignements personnels et que des mécanismes de recours robustes et accessibles soient mis en place. L'efficacité de la sécurité repose sur la collecte d'information pertinente seulement.

5.3 Collaboration avec les institutions fédérales

Au cours du dernier exercice financier, le Commissariat a continué à participer à un dialogue constructif avec le plus grand nombre possible d'institutions parmi les 250 institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels*.

Nous avons pour objectifs d'aider les organisations à régler les questions en suspens liées à la protection de la vie privée, de mieux comprendre nos attentes quant aux évaluations des facteurs relatifs à la vie privée et de promouvoir l'importance d'aviser le Commissariat des atteintes à la protection des renseignements personnels.

Pour leur part, les ministères ont généralement démontré une volonté à travailler avec nous afin de mieux protéger les renseignements personnels des Canadiennes et Canadiens.

5.3.1 AIDE POUR LES ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Une des activités importantes du Commissariat est l'examen des évaluations des facteurs relatifs à la vie privée. Par l'examen de ces évaluations de programmes et initiatives du gouvernement qui utilisent les renseignements personnels des Canadiennes et des Canadiens, nous sommes en mesure d'évaluer la conformité des institutions à la *Loi sur la protection des renseignements personnels* (parmi d'autres exigences juridiques et stratégiques). Nous pouvons aussi offrir des conseils pertinents sur la façon de concevoir les programmes pour assurer une meilleure protection de la vie privée.

Les détails de nombreuses initiatives que nous étudions ne sont pas rendus publics en raison de leur nature délicate. Toutefois, par l'entremise du processus d'examen, nous nous assurons, au nom du public, que le gouvernement respecte le droit à la vie privée des Canadiennes et des Canadiens.

NOUVELLE DIRECTIVE

Pour nous acquitter de cette tâche importante, nous poursuivons nos efforts de collaboration avec les institutions fédérales afin de les aider à s'adapter à la nouvelle directive sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor.

Nous voulons également expliquer ce que nous recherchons lorsque nous analysons les évaluations afin de veiller à ce que du contenu important ne soit pas négligé et que des évaluations approfondies continuent d'être menées.

Au cours du dernier exercice financier, nous avons mené des consultations avec la GRC sur sa politique provisoire sur l'aide aux victimes, avec

Directive du Secrétariat du Conseil du Trésor sur l'évaluation des facteurs relatifs à la vie privée

Une nouvelle directive du Secrétariat du Conseil du Trésor, en vigueur depuis le 1er avril 2010, introduit le concept d'évaluation des facteurs relatifs à la vie privée « de base », qui représente le niveau minimal d'analyse requise pour certains dossiers à risque faible. Cependant, nous croyons qu'une telle évaluation pourrait être inadéquate. En effet, nous avons reçu des dossiers qui ne pouvaient être examinés sans l'obtention d'information additionnelle.

Plus d'une année après la mise en œuvre de la Directive, les fonctionnaires qui doivent préparer des évaluations des facteurs relatifs à la vie privée attendaient encore que le Secrétariat du Conseil du Trésor publie des lignes directrices officielles supplémentaires. Sans de tels documents clés, la qualité des analyses n'est pas uniforme.

Citoyenneté et Immigration Canada relativement à la collecte accrue de renseignements biométriques de certains immigrants, réfugiés et demandeurs de visa, et avec l'Agence des services frontaliers du Canada pour ce qui est de la renégociation de l'entente sur le Système d'information préalable sur les voyageurs/Dossier passager entre le Canada et l'Europe.

Ces consultations précèdent habituellement la réception d'une évaluation des facteurs relatifs à la vie privée, qui aide à veiller à ce que les risques pour la protection de la vie privée soient cernés, évalués et atténués avant la mise en œuvre d'un programme.

ATELIER ET DOCUMENT SUR NOS ATTENTES

En mars 2011, nous avons été l'hôte du deuxième atelier annuel sur les évaluations des facteurs relatifs à la vie privée, auquel ont assisté plus de 100 représentants de 40 institutions fédérales. Cet événement nous a permis de donner des conseils à un public diversifié sur la façon d'effectuer des évaluations des facteurs relatifs à la vie privée.

Nos attentes : un guide pour la présentation d'évaluations des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada

Nous avons profité de l'atelier pour présenter un nouveau document d'orientation, intitulé *Nos attentes : un guide pour la présentation d'évaluations des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada*.

Le document, qui a été affiché sur notre site Web à titre de complément à la nouvelle directive du Secrétariat du Conseil du Trésor, explique le type de renseignements et la portée de l'information et de l'analyse que nous désirons voir dans les évaluations des facteurs relatifs à la vie privée.

Pour les initiatives pouvant porter davantage atteinte à la vie privée, par exemple, nous demandons aux institutions de démontrer le besoin, la proportionnalité et l'efficacité de la mesure proposée et d'expliquer si une mesure moins envahissante pourrait être utilisée.

Une fois que cet examen en quatre parties a été fait et que la collecte et l'utilisation des renseignements personnels ont été justifiées, nous demandons aux institutions de démontrer la sécurité de l'information qu'ils souhaitent recueillir.

Plus particulièrement, nous encourageons les institutions à analyser les risques de leurs propositions en fonction des 10 principes universels relatifs à la protection de la vie privée et à l'équité dans le traitement de l'information du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation. Ces principes ont trait notamment à la responsabilité, à la limitation de la collecte, au consentement, aux mesures de sécurité et à l'accès aux renseignements personnels.

Entre-temps, nous continuons d'explorer d'autres façons d'élargir nos efforts de rayonnement au sein de la fonction publique et nous avons demandé de la rétroaction de la part des participants à l'atelier afin de peaufiner nos présentations sur les évaluations des facteurs relatifs à la vie privée.

SIMPLIFIER LE PROCESSUS

Nous avons continué cette année à simplifier le processus d'examen des évaluations et à concentrer nos ressources sur les initiatives qui présentent le plus de risques au droit à la vie privée des Canadiennes et Canadiens. Par exemple, nous avons continué à mettre au point notre processus de tri et nous l'avons officialisé.

Chaque évaluation des facteurs relatifs à la vie privée que nous recevons est examinée par un agent d'examen afin d'évaluer le caractère délicat de l'information recueillie, la nature des risques découlant de l'initiative, le nombre de Canadiennes et de Canadiens touchés par le programme ou l'activité et pour déterminer si l'initiative appartient à l'un des quatre secteurs qui, selon nous, auront le plus de répercussions sur le droit à la vie privée — la sécurité publique, les technologies de l'information, les renseignements génétiques et la protection de l'intégrité de l'identité.

Bien que nous lisons et évaluons tous les dossiers reçus, nous effectuons des examens plus approfondis lorsque, à notre avis, une initiative pose des risques importants pour la vie privée ou soulève des questions plus vastes liées aux droits de la personne ou à la société en général. Dans ces cas, nous fournissons des recommandations détaillées aux ministères et nous effectuons un suivi afin de veiller à l'atténuation des risques.

5.3.2 FORUM SUR LES PRATIQUES RELATIVES À LA PROTECTION DE LA VIE PRIVÉE

Le 15 mars, le Commissariat a présidé le premier Forum sur les pratiques relatives à la protection de la vie privée. Cette séance a été l'occasion pour les fonctionnaires fédéraux de partager leur expérience et leur savoir liés à l'amélioration de la protection de la vie privée dans le contexte de leur ministère.

En tout, 64 employés provenant de 15 ministères et organismes se sont inscrits à la séance.

Des représentants de quatre institutions fédérales ont décrit les outils et les processus qu'ils ont mis en œuvre dans leur environnement de travail respectif. Ces présentations ont été suivies de discussions en petits groupes auxquelles ont pris part les participants désireux d'examiner plus en profondeur des sujets ou des approches spécifiques.

Le Forum a traité de questions importantes comme les structures de gouvernance de la protection de la vie privée, les protocoles en matière de gestion des atteintes à la protection des renseignements personnels, les outils disponibles en ligne pour préparer de meilleures évaluations des facteurs relatifs à la vie privée et l'élaboration d'une politique interne pour l'utilisation des médias sociaux.

Les présentations ont été enregistrées sur vidéo en vue de leur affichage sur GCPEDIA, un outil de travail collaboratif des fonctionnaires fédéraux.

5.3.3 ÉCOLE DE LA FONCTION PUBLIQUE DU CANADA

Le bon fonctionnement de notre système démocratique de gouvernement repose sur une fonction publique qui comprend ses obligations à l'égard de la protection des renseignements personnels des Canadiennes et Canadiens qui se trouvent en sa possession. C'est la raison pour laquelle le Commissariat continue de travailler avec l'École de la fonction publique du Canada pour trouver des façons de promouvoir la protection des renseignements personnels parmi les employés fédéraux.

En octobre 2010, la commissaire a présidé une discussion informelle, qui a connu un franc succès, dans les locaux du fournisseur commun de services d'apprentissage pour la fonction publique fédérale, situés à Gatineau, au Québec. Elle y a décrit comment intégrer les considérations en matière de protection de la vie privée aux priorités plus vastes du gouvernement et elle a présenté les priorités, les activités et les approches du Commissariat, qui visent le renforcement des mesures de protection de la vie privée au sein du gouvernement.

De plus, l'École a accepté d'offrir des ateliers sur la protection de la vie privée dans le cadre de la Série d'excellence en gestion. Les ateliers sont conçus pour aller au-delà de la gestion quotidienne des bases de données et des renseignements personnels, et portent principalement sur les considérations clés que doivent prendre en compte les hauts responsables de l'élaboration des politiques lorsqu'ils créent de nouveaux programmes et services qui pourraient avoir des répercussions sur le droit à la vie privée des Canadiennes et Canadiens.

Nous travaillons aussi avec le centre d'apprentissage pour élaborer des ateliers sur la protection de la vie privée dans le cadre de sa nouvelle série de séminaires pour les sous-ministres, qui donnera également l'occasion aux hauts fonctionnaires d'institutions fédérales de se rencontrer et de discuter des nouveaux enjeux.

Nous souhaitons toujours examiner les cours offerts par l'organisation, afin de veiller à ce que les principes essentiels en matière de protection de la vie privée soient bien compris par tous les fonctionnaires qui en ont besoin dans le cadre de leurs activités quotidiennes.

5.4 Actions en justice

En vertu de la *Loi sur la protection des renseignements personnels*, la commissaire à la protection de la vie privée peut demander une audience à la Cour fédérale ou comparaître devant celle-ci lorsqu'une institution fédérale rejette une demande d'accès à des renseignements personnels déposée par une personne. Notre participation à ces audiences est décrite à la section 3.4.

De temps à autre, le Commissariat peut demander de participer à titre d'intervenant dans d'autres affaires devant les cours ou autres tribunaux, afin de clarifier des questions liées à l'interprétation de certaines dispositions de la *Loi sur la protection des renseignements personnels* ou d'autres questions portant sur le droit à la vie privée ou sur la protection des renseignements personnels. De plus, le Commissariat peut parfois faire l'objet de demandes de contrôle judiciaire.

Voici des résumés des affaires auxquelles nous avons participé en 2010-2011. Conformément à l'esprit de notre mandat, nous ne publions pas le nom des plaignants. Le numéro de dossier et le nom des institutions mises en cause sont toutefois fournis.

5.4.1 *INSTITUT PROFESSIONNEL DE LA FONCTION PUBLIQUE DU CANADA c. AGENCE DU REVENU DU CANADA* 2011 CRTFP 34

Dans cette affaire, une employée de l'Agence du revenu du Canada, dont le lieu de travail syndiqué était représenté par l'Institut professionnel de la fonction publique du Canada, s'opposait à ce que son employeur fournisse ses coordonnées à la maison au syndicat, conformément à une ordonnance émise en juillet 2008 par la Commission des relations de travail dans la fonction publique (CRTFP). L'employée était une « cotisante Rand », soit une employée qui décide de ne pas être membre du syndicat, mais qui doit toutefois en payer les cotisations.

Le syndicat et l'employeur ont conclu une entente en vertu de laquelle les renseignements personnels des employés de l'unité de négociation peuvent être communiqués à l'employeur. Cette entente a été approuvée par la CRTFP dans son ordonnance de juillet 2008.

Insatisfaite de l'entente, l'employée a déposé en 2009 une demande de contrôle judiciaire liée à l'ordonnance devant la Cour d'appel fédérale. La demande était fondée sur la protection des renseignements personnels et l'équité de la procédure.

En février 2010, la Cour d'appel fédérale a accepté la demande de l'employée et a retourné l'affaire à la CRTFP pour réexamen. Dans sa décision, la Cour fédérale

précisait que le Commissariat devrait être avisé de cette nouvelle audience et recevoir le statut d'intervenant. Par conséquent, le Commissariat a participé à titre d'intervenant aux audiences de réexamen qui ont eu lieu devant la CRTFP en novembre 2010.

Nous étions d'avis que le syndicat n'a pas besoin des coordonnées à la maison d'un employé pour s'acquitter de ses obligations en vertu de la loi, c'est-à-dire pour informer tous les membres d'une unité de négociation de la tenue d'un vote de grève.

La CRTFP a rendu sa décision le 23 mars 2011 et concluait que l'employeur pouvait fournir au syndicat les coordonnées à la maison d'un employé sans le consentement de celui-ci, en vertu de la *Loi sur les relations de travail dans la fonction publique* et de la *Loi sur la protection des renseignements personnels*.

Cependant, l'arbitre a apporté diverses modifications visant à renforcer la protection des renseignements personnels à l'entente d'échange de renseignements contestée entre l'employeur et le syndicat.

La CRTFP a de plus reconnu que, dans le contexte de cette affaire, il y avait des lacunes dans la protection législative des renseignements personnels des employés syndiqués. Compte tenu des activités du syndicat, la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* ne s'appliquaient pas.

En avril 2011, à la suite de l'audience de réexamen, l'employée a encore une fois déposé une demande pour un contrôle judiciaire devant la Cour fédérale pour ce qui est de l'ordonnance de la CRTFP. L'affaire a été transférée à la Cour d'appel fédérale le 5 mai 2011 suivant une ordonnance de la Cour fédérale.

5.4.2 *X c. COMMISSION DE LA FONCTION PUBLIQUE NO DE DOSSIER DE LA COUR FÉDÉRALE : T-1659-08*

Dans un cas de longue date dont les progrès ont été expliqués dans des rapports annuels antérieurs, la Commission de la fonction publique a mené une enquête sur une personne qui avait présumément pris part à des activités politiques inappropriées pendant qu'elle travaillait pour la fonction publique fédérale.

À la suite d'une enquête interne sur cette affaire, la Commission de la fonction publique a décidé qu'elle afficherait un résumé de ses constatations sur Internet, conformément à ses pratiques de l'époque. La personne a estimé que cela représentait une atteinte injustifiée de son droit à la vie privée et a déposé une demande de contrôle judiciaire devant la Cour fédérale.

L'affaire soulevait des questions liées à la communication de renseignements personnels sur Internet et sur la mesure dans laquelle le principe des audiences publiques s'applique aux tribunaux administratifs comme la Commission de la fonction publique.

La commissaire à la protection de la vie privée a demandé et reçu le titre d'intervenante, afin d'aider la Cour sur certaines questions juridiques soulevées dans la demande.

Quatre autres institutions fédérales ont aussi obtenu qualité d'intervenant — la Commission des relations de travail dans la fonction publique, le Tribunal de la dotation de la fonction publique, la Commission d'examen des plaintes concernant la police militaire et l'Office des transports du Canada.

Le demandeur a finalement annulé sa demande.

5.4.3 *X c. COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA ET COMMISSAIRE À L'INFORMATION DU CANADA NO DE DOSSIER DE LA COUR FÉDÉRALE : DC-09-88-JR*

Comme nous l'avons mentionné dans le rapport annuel de l'année dernière, il s'agissait d'une demande de contrôle judiciaire, déposée à la Cour divisionnaire de la Cour supérieure de justice de l'Ontario, dans laquelle le demandeur souhaitait obtenir une ordonnance de mandamus, exigeant que le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information du Canada réalisent des enquêtes concernant des plaintes déposées par le demandeur auprès des deux commissariats. La demande a finalement été rejetée le 22 janvier 2010.

Toutefois, l'affaire s'est poursuivie au cours du dernier exercice financier, lorsque le plaignant a demandé que la Cour d'appel de l'Ontario infirme la décision de rejeter la demande.

La Cour d'appel a rappelé au demandeur qu'il lui fallait suivre la procédure appropriée en demandant à la Cour divisionnaire de l'Ontario l'annulation de l'ordonnance, mais elle a finalement ajourné l'audience à une date indéterminée.

Le demandeur a voulu interjeter appel de la décision de la Cour d'appel, mais n'a pas réussi à le faire. Il n'a toujours pas présenté l'affaire à la Cour divisionnaire de l'Ontario.

5.5 Développement du savoir

5.5.1 RECHERCHES COMMANDÉES

Nous avons commandé plusieurs rapports de recherche au cours de la dernière année. La plupart examinaient les facteurs pouvant nuire à l'intégrité et à la protection de l'identité personnelle, une de nos priorités stratégiques. Parmi les rapports de recherche directement pertinents pour le secteur public, mentionnons notamment :

- *Enquête qualitative auprès des agents de l'AIPRP*

Nous avons chargé Phoenix Strategic Perspectives Inc. d'interviewer certains agents fédéraux responsables de l'accès à l'information et de la protection des renseignements personnels (AIPRP) pour en savoir plus au sujet de leurs principales préoccupations. Il s'est avéré que celles-ci comprenaient la préparation adéquate d'évaluations des facteurs relatifs à la vie privée et la difficulté de protéger les renseignements personnels à un moment où le gouvernement recueille plus de données que jamais.

La capacité croissante du gouvernement à surveiller l'activité des citoyens au moyen de technologies comme les systèmes de positionnement global (GPS), la surveillance de la circulation, les inforobots de recherche Web et le contrôle des sites des médias sociaux a été désignée comme étant un nouvel enjeu important.

Au nombre des autres enjeux mentionnés par les répondants figuraient la difficulté de trouver un équilibre entre le droit à la vie privée et le besoin d'assurer la sécurité publique et celle d'assurer la protection de la vie privée tout en utilisant les médias sociaux.

Cette enquête permettra au Commissariat de mieux comprendre le contexte dans lequel ces agents travaillent, et comment il peut continuer de les appuyer.

- *Recherche sur la protection de la vie privée dans les pays en développement*

M. Gus Hosein, attaché supérieur de recherches invité à la London School of Economics and Political Science, dont les intérêts de recherche portent sur la réglementation, les libertés civiles et les politiques en matière de technologie, constate que presque toutes les déclarations internationales sur les droits comprennent des mesures explicites de protection de la vie privée.

On a souvent affirmé que, pour les pays en développement, le développement économique est plus important que les droits de la personne comme le droit à la vie privée. Cependant, on peut soutenir que le contraire est vrai, étant donné que les droits de la personne sont essentiels à la bonne gouvernance et à l'efficacité des gouvernements.

Le rapport explique que les pays en développement sont des chefs de file en ce qui concerne l'adoption et l'élaboration de nouvelles pratiques de surveillance. Les systèmes d'identification nationale, la surveillance des déplacements et des communications, les bases de données génétiques et les systèmes de cybersanté gagnent tous du terrain dans ces pays.

Toutefois, le rapport souligne que les lois sur la protection des données de ces pays accusent un retard.

L'auteur fait observer que le Centre de recherches pour le développement international du Canada a été un chef de file mondial bénéficiant d'un appui sans précédent en matière de renforcement de la capacité relative à la protection de la vie privée dans les pays en développement.

D'autre part, le Commissariat a été reconnu comme étant très actif sur le plan international relativement à la promotion et à la protection de la vie privée, notamment en participant à des groupes comme l'APEC, le Forum ibéro-américain des autorités de protection des données et l'Association francophone des autorités de protection des données personnelles.

- *Examen dirigé de la documentation sur les systèmes de gestion de l'identité*

En juin 2010, le gouvernement fédéral a annoncé la création du Groupe de travail sur l'examen du système de paiements dont le mandat est d'examiner le système actuel que les Canadiennes et Canadiens utilisent pour acheter des produits et des services en ligne. Le Groupe de travail doit faire rapport au ministère des Finances d'ici la fin de 2011.

En prévision du rapport de consultation du Groupe de travail, nous avons commandé un examen de la documentation sur les systèmes fédérés de gestion de l'identité.

L'examen, préparé par Jennifer Barrigar, spécialiste des questions relatives à la protection de la vie privée et à la technologie et ancienne avocate au sein de la Direction des services juridiques du Commissariat, conclut que l'authentification d'un tiers et les marqueurs d'identité fiables en ligne peuvent réduire le risque de vol d'identité et de fraude et, ce faisant, améliorer la confiance des gens à l'égard du commerce électronique.

Ces mêmes caractéristiques, mises en œuvre de manière inadéquate, pourraient faciliter, plutôt que prévenir, l'accès criminel aux renseignements personnels.

De la même façon, le fait d'avoir un seul inventaire de données et un seul mot de passe ou jeton d'accès peut accroître la sécurité, mais des lacunes dans la mise en œuvre de

telles mesures de sécurité pourraient permettre un accès non autorisé à un ensemble de données sans précédent.

L'examen propose que de tels systèmes de gestion de l'identité, qui sont également devenus plus courants au sein du gouvernement, soient assujettis à une réglementation souple axée sur l'information plutôt que sur la technologie utilisée. Il est également essentiel que cela se fasse au su des utilisateurs et avec leur consentement.

5.5.2 TABLES RONDES DE L'INSTITUT D'ADMINISTRATION PUBLIQUE

Le Commissariat a octroyé des fonds à l'Institut d'administration publique du Canada afin qu'il mène des tables rondes sur l'utilisation des médias sociaux au sein du gouvernement, y compris les questions connexes relatives à la protection de la vie privée. Cinq tables rondes ont eu lieu au cours de l'année à Edmonton, Victoria, Toronto, Kingston, en Ontario, et Ottawa, attirant des fonctionnaires des administrations fédérale, provinciales et municipales, ainsi que des représentants du milieu universitaire.

Les tables rondes ont établi que les outils des médias sociaux peuvent à la fois aider les institutions à mieux s'acquitter de leur mission, tout en facilitant un style de gestion plus efficace. Ces outils permettent de réduire les coûts, d'accroître la productivité et de contribuer à la satisfaction des employés et des citoyens. En plus, ils peuvent être utilisés efficacement sans contrevenir aux règlements sur la protection des renseignements personnels.

Les tables rondes ont relevé que la plupart des gouvernements ont maintenant des médias sociaux internes, comme GCPEDIA au sein du gouvernement du Canada. Toutefois, ces médias ne sont pas intégrés avec ceux d'autres instances. Les recommandations des tables rondes sont notamment les suivantes :

- Une source centrale intergouvernementale d'information et de réseautage. Les fonctionnaires pourraient consulter un tel site pour voir les lignes directrices et les analyses de rentabilisation élaborées par d'autres instances. Ils pourraient aussi s'en servir pour établir des liens avec d'autres personnes travaillant à des questions similaires, afficher des problèmes et partager des solutions.

- Des travaux supplémentaires sont nécessaires pour clarifier la façon dont les gouvernements peuvent utiliser les médias sociaux pour rendre les organisations du secteur public plus productives et mieux en mesure de faire face aux défis complexes du monde actuel, tout en améliorant l'élaboration et la mise en œuvre des politiques.

La recherche de l'Institut visait à améliorer la compréhension du Commissariat quant aux répercussions de l'utilisation des médias sociaux au sein du gouvernement, notamment en ce qui concerne les facteurs de réussite, l'utilisation d'outils d'établissement de rapports et les analyses coûts-avantages.

Le travail visait également à éclairer la mise en œuvre et l'utilisation des médias sociaux au sein d'autres ministères, permettant ainsi au Commissariat de s'acquitter de son mandat en matière d'éducation et de sensibilisation du public.

L'Institut invite les intervenants à formuler des commentaires sur le rapport, lequel sera rendu public.

5.5.3 LA FRANCOPHONIE

Le Commissariat continue d'être un membre actif de l'*Association francophone des autorités de protection des données personnelles* (AFAPDP), une association œuvrant dans les pays francophones. Créée à Montréal en 2007, l'Association a pour mandat de promouvoir la protection des données personnelles en renforçant la capacité de ses membres et en identifiant les nouvelles menaces pour le droit à la vie privée.

Étant donné que plusieurs des 24 membres de l'Association sont des États en développement, la participation du Commissariat à la protection de la vie privée du Canada contribue de manière importante au renforcement des pratiques de bonne gouvernance dans ces pays.

Lors de l'assemblée générale annuelle de l'Association à Paris en novembre 2010, la commissaire adjointe à la protection de la vie privée, Chantal Bernier, a décrit l'évolution de la protection des données personnelles au Canada, ainsi que les principes de gouvernance essentiels à une surveillance indépendante de la protection de la vie privée.

L'année à venir

Le présent rapport explique en détail comment les vérifications, les enquêtes, les examens des évaluations des facteurs relatifs à la vie privée et nos interactions avec le Parlement, la fonction publique et les citoyens ont servi en 2010-2011 à renforcer la protection des renseignements personnels dans le secteur public.

Cependant, lorsque nous regardons vers l'année à venir et au-delà, il est évident que les défis ne feront qu'augmenter.

Prenons, par exemple, la question de la cybersécurité, une grande préoccupation pour le gouvernement du Canada et, en fait, pour les gouvernements du monde entier.

Certains aspects de la cybersécurité renforcée, comme les mesures visant à mieux protéger les renseignements personnels dans le cyberespace, sont cruciaux pour la protection de la vie privée et sont, par conséquent, des initiatives gouvernementales que l'on accueille favorablement.

Par contre, certains autres aspects — plus particulièrement l'élargissement des pouvoirs policiers dans l'environnement Internet — soulèvent toujours des préoccupations. Nous continuerons d'exprimer notre point de vue selon lequel ces soi-disant mesures sur l'accès légal doivent respecter le droit fondamental à la vie privée.

Aujourd'hui, les Canadiennes et Canadiens sont habitués à des communications sécurisées qui leur permettent de s'exprimer, de créer, de partager et d'innover. Ils s'attendent à ce que leur gouvernement leur offre des services de manière confidentielle et fiable, et à ce qu'il soit un défenseur irréprochable de leurs renseignements personnels.

En même temps, ils s'attendent aussi à ce que leur gouvernement soit ouvert et réceptif, et non pas paralysé par l'obsession de la sécurité.

Au cours de l'année à venir, le Commissariat travaillera à faire en sorte que les faiblesses des réseaux informatiques et des systèmes gouvernementaux en matière de sécurité soient confrontées, mais dans le respect de la loi — que ce soit le droit à la vie privée

découlant de la *Charte canadienne des droits et libertés*, les dispositions de la *Loi sur la protection des renseignements personnels*, ou les dispositions relatives à la protection de la vie privée du *Code criminel*.

Au chapitre des grands enjeux, l'un des principaux risques pour la protection de la vie privée au 21e siècle demeure l'échange d'information entre ministères, ordres de gouvernement et autres États. Un autre défi majeur en ce qui concerne la gouvernance et le contrôle des pratiques relatives au traitement des renseignements personnels est de faire en sorte que les mécanismes de surveillance et d'examen soient mûrement réfléchis, qu'ils disposent de ressources suffisantes et qu'ils soient assortis de conséquences importantes.

Ainsi, pour tous les nouveaux programmes et initiatives légales nécessitant une surveillance, un contrôle ou un examen, le Commissariat continuera de plaider en faveur de la discussion ouverte, de normes élevées de protection de la vie privée, de mécanismes d'examen solides, d'une surveillance judiciaire forte et de procédures de recours claires, ainsi que pour un engagement ferme à l'égard de l'application régulière de la loi et de la primauté du droit.

AU SERVICE DE LA POPULATION CANADIENNE

Plus précisément, nous produirons en 2011-2012 un rapport sur les grandes préoccupations liées à un ensemble de neuf évaluations des facteurs relatifs à la vie privée que nous avons reçues depuis 2007 concernant le régime canadien de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes.

Tous les risques et les enjeux communs ou systémiques relatifs à la protection des renseignements personnels que nous soulèverons nous aideront à éclairer notre prochain examen du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE). Nous sommes tenus de mener un tel examen annuellement, conformément à la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*. Le prochain examen visera également les mesures que le CANAFE a mises en œuvre pour donner suite aux conclusions de la vérification complète que nous avons effectuée en 2009.

Nous terminerons également notre vérification d'Anciens Combattants Canada, lancée au cours du dernier exercice après qu'une enquête sur une plainte ait révélé de graves problèmes systémiques au sein de ce ministère. Notre vérification, qui devrait être terminée au cours de l'hiver 2011-2012, déterminera si le Ministère donne suite aux recommandations que nous avons formulées dans notre rapport des conclusions découlant de cette enquête, et s'il met en œuvre le plan d'action en 10 points qu'il a

élaboré en vue de renforcer ses politiques et ses pratiques en matière de protection de la vie privée.

Dans l'année à venir, nous continuerons de renforcer nos processus internes et notre capacité à nous acquitter de notre mandat, à l'aide des meilleures pratiques actuelles.

Ainsi, par exemple, nous prévoyons analyser l'intégralité de plus de 500 évaluations des facteurs relatifs à la vie privée qui ont été présentées au Commissariat depuis 2002, afin de produire des statistiques sur la nature des dossiers que nous recevons, les types d'enjeux auxquels nous sommes confrontés et les ministères et organismes qui soumettent la plupart de ces dossiers.

Nous sommes convaincus que ces données appuieront le travail du Commissariat dans son ensemble, tout en éclairant la fonction publique, le Parlement et la population canadienne sur la valeur du processus d'examen des évaluations des facteurs relatifs à la vie privée.

Parce que nous reconnaissons que le paysage changeant de la protection de la vie privée peut présenter de nombreuses difficultés pour les fonctionnaires à qui ont été confiés les renseignements personnels des Canadiennes et des Canadiens, nous avons également l'intention de mener des activités de sensibilisation. À cette fin, nous prévoyons établir un espace de travail de collaboration sur GCconnex, le site de réseautage social à l'intention des fonctionnaires fédéraux.

Nous avons l'intention de tenir davantage de séances pratiques afin d'aider les institutions à préparer des évaluations des facteurs relatifs à la vie privée. Nous avons sollicité des idées de la part des participants lors de notre dernier atelier sur l'évaluation des facteurs relatifs à la vie privée, et nous utiliserons les résultats de notre récent sondage auprès des coordonnateurs fédéraux de l'accès à l'information et de la protection des renseignements personnels afin d'essayer de mieux répondre à leurs besoins.

Grâce à notre engagement renouvelé de mieux servir les Canadiennes et les Canadiens, nous continuerons également de sensibiliser les citoyens du Canada aux questions relatives à la protection de la vie privée, à la protection des renseignements personnels et au droit d'accès à ces renseignements.

Nous y parviendrons en renforçant davantage notre capacité à répondre de façon rapide et efficace à leurs demandes de renseignements et à leurs plaintes. Nous y parviendrons également au moyen d'événements publics, de recherche opportune, de discussions ouvertes, de séminaires et d'une présence en ligne accrue.

Les enjeux liés à la collecte et à la protection des renseignements personnels par le gouvernement deviennent de plus en plus complexes. Par conséquent, pour conserver intacte la confiance des citoyens à notre endroit, nous devons faire en sorte que ceux-ci puissent participer à la discussion, laquelle doit être axée sur ce qu'ils vivent.

La protection de la vie privée est un élément beaucoup trop essentiel à notre société et au maintien de nos valeurs démocratiques pour devenir un enjeu qui ne concerne que le gouvernement.

ANNEXE 1
DÉFINITIONS

TYPES DE PLAINTES

1. Accès

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

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

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

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

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

2. Protection des renseignements personnels

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

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

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

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

3. Délais

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

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

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

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

1. Conclusions d'enquêtes

Fondée : L'institution fédérale n'a pas respecté les droits d'une personne aux termes de la *Loi sur la protection des renseignements personnels*. Cette catégorie comprend les conclusions auparavant désignées **fondées et résolues**, c'est-à-dire où les allégations étaient corroborées par l'enquête et l'institution fédérale acceptait de prendre des mesures correctives afin de remédier à la situation.

Non fondée : L'enquête n'a pas permis de déceler les éléments de preuve qui suffisent à conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant en vertu de la *Loi sur la protection des renseignements personnels*.

Résolue : Après une enquête approfondie, le Commissariat a participé à la négociation d'une solution satisfaisant les deux parties. Cette conclusion est réservée aux plaintes qu'on pourrait difficilement qualifier de fondées du fait que la situation relève essentiellement d'une mauvaise communication ou d'un malentendu.

2. Autres décisions

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

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

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

ANNEXE 2

Processus d'enquête en vertu de la *Loi sur la protection des renseignements personnels*

Demande de renseignements :
Une personne communique avec le CPVP par lettre, par téléphone ou en personne pour déposer une plainte relative à une infraction à la *Loi*. Les personnes qui communiquent par téléphone ou en personne doivent par la suite présenter leurs allégations par écrit.

↓

Analyse initiale :
Le registraire des plaintes examine l'affaire en cause afin de déterminer si elle constitue bel et bien une plainte, c.-à-d. de déterminer si les faits allégués pourraient contrevenir à la *Loi*, ainsi que le moyen le plus efficace de la résoudre.

Une personne peut déposer une plainte se rapportant à toute question énoncée à l'article 29 de la *Loi sur la protection des renseignements personnels* – par exemple, le refus d'une institution de communiquer à une personne les renseignements personnels qu'elle détient à son sujet, ou un retard inacceptable dans la communication de ces renseignements; la collecte, l'utilisation ou la communication inappropriée de renseignements personnels; des erreurs dans les renseignements personnels qu'une institution utilise ou communique.

↓

Plainte?

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

Oui :
Un enquêteur est affecté au dossier.

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

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

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

↓

Analyse (suite)

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

Résolue? (suite)

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

Analyse :

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

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

Résolue?

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

Conclusion :

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

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

Les conclusions possibles sont les suivantes :

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

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

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

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

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

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

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

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

ANNEXE 3
Demandes de renseignements, plaintes et enquêtes en vertu de la *Loi sur la protection des renseignements personnels*, du 1er avril 2010 au 31 mars 2011

STATISTIQUES SUR LES DEMANDES DE RENSEIGNEMENTS

Demandes de renseignements liées à la *Loi sur la protection des renseignements personnels* reçues

Demandes téléphoniques :	1 046
Autres* :	898
Total :	1 944

Demandes de renseignements générales† reçues

Demandes téléphoniques :	1 974
Autres :	214
Total :	2 188

Réponses aux demandes de renseignements liées à la *Loi sur la protection des renseignements personnels*

Demandes téléphoniques :	1 034
Par écrit :	825
Total :	1 859

Réponses aux demandes de renseignements générales†

Demandes téléphoniques :	1 972
Par écrit :	211
Total :	2 183

* Peut comprendre les demandes de renseignements par courrier, courriel et télécopieur ou en personne.

† Demandes de renseignements concernant des enjeux ne pouvant être liés exclusivement à la *Loi sur la protection des renseignements personnels* ou à la *Loi sur la protection des renseignements personnels et les documents électroniques*..

PLAINTES REÇUES PAR TYPE DE PLAINTE

Type de plainte	Nombre		Total	Pourcentage	Total par type de plainte
	Règlement rapidement	Plainte officielle			
Accès	28	293	321	45	**Accès 328**
Correction/ annotation	2	4	6	1	
Frais	0	1	1	0.1	
Correction – délais	0	1	1	0.1	**Délais 251**
Délais	3	231	234	33	
Avis de prorogation	0	16	16	2	
Collecte	7	5	12	2	**Protection des renseignements personnels 129**
Langue	0	3	3	1	
Conservation et retrait	0	9	9	1	
Utilisation et communication	36	69	105	15	
Total	**76**	**632**	**708**	**100**	**708**

Le plus souvent, les plaintes déposées au Commissariat en 2010-2011 portaient sur l'accès aux renseignements personnels détenus par les ministères ou les organismes gouvernementaux. Ces plaintes comptaient pour un total combiné de 328, ou 46 % de toutes les plaintes reçues au Commissariat. Le nombre de plaintes liées à l'accès a augmenté de 31 % par rapport à 2009-2010.

La deuxième raison la plus fréquente pour laquelle les personnes ont déposé des plaintes au Commissariat concernait le temps que les ministères et organismes ont pris pour répondre aux demandes d'accès. Le Commissariat a reçu 251 plaintes liées aux délais, soit un peu plus du tiers (35 %) des cas à traiter. Cela représentait une diminution de 14 % par rapport à l'année précédente.

Les plaintes liées à la protection des renseignements personnels, y compris les problèmes liés à la collecte, à l'utilisation, à la communication, à la conservation et au retrait des renseignements personnels, constituaient un total de 129 plaintes, ce qui représente 18 % du total. Cela ne correspondait qu'à une légère (7 %) augmentation par rapport à 2009-2010, lorsque le Commissariat a reçu 122 plaintes de cette catégorie.

Voir l'annexe 1 pour les définitions des types de plaintes.

LES 10 INSTITUTIONS AYANT FAIT L'OBJET DU PLUS GRAND NOMBRE DE PLAINTES

Organisation	Accès			Délais			Protection des renseignements personnels			Total
	Règlement rapide	Plainte officielle	Total	Règlement rapide	Plainte officielle	Total	Règlement rapide	Plainte officielle	Total	
Service correctionnel du Canada	7	87	**94**	1	158	**159**	11	12	**23**	**276**
Gendarmerie royale du Canada	11	46	**57**	0	8	**8**	1	9	**10**	**75**
Défense nationale	0	42	**42**	0	19	**19**	1	3	**4**	**65**
Agence du revenu du Canada	0	29	**29**	0	16	**16**	1	7	**8**	**53**
Agence des services frontaliers du Canada	0	15	**15**	0	9	**9**	1	4	**5**	**29**
Société canadienne des postes	2	5	**7**	0	3	**3**	7	10	**17**	**27**
Ressources humaines et Développement des compétences Canada	3	9	**12**	0	4	**4**	2	7	**9**	**25**
Citoyenneté et Immigration Canada	0	12	**12**	0	2	**2**	0	2	**2**	**16**
Service canadien du renseignement de sécurité	1	13	**14**	0	2	**2**	0	0	**0**	**16**
Anciens Combattants Canada	3	2	**5**	0	0	**0**	0	10	**10**	**15**
Autres	3	38	**41**	2	27	**29**	19	22	**41**	**111**
Total	**30**	**298**	**328**	**3**	**248**	**251**	**43**	**86**	**129**	**708**

Ces 10 institutions comptent pour 84 % de toutes les plaintes reçues en 2010-2011. Cette proportion n'a presque pas changé par rapport à celle de 85 % mesurée pour les 10 ministères et organismes ayant fait l'objet du plus grand nombre de plaintes en 2009-2010.

Le nombre de plaintes déposées contre une institution n'est pas nécessairement un indicateur permettant de conclure que ses pratiques ne sont pas conformes à la *Loi sur la protection des renseignements personnels*. En raison de leur mandat, certaines institutions détiennent une quantité considérable de renseignements personnels. Elles sont donc plus susceptibles de recevoir de nombreuses demandes d'accès à ces renseignements personnels, ce qui peut donner lieu à des plaintes subséquentes sur les pratiques de l'institution en matière de collecte, d'utilisation, de communication, de conservation ou de retrait des renseignements personnels, ou sur la manière dont l'institution donne accès à ces renseignements.

PLAINTES REÇUES PAR INSTITUTION

Institution	Règlement rapide	Plaintes officielles	Total
Affaires étrangères et Commerce international Canada	1	7	**8**
Affaires indiennes et du Nord Canada	1	0	**1**
Agence canadienne d'inspection des aliments	1	7	**8**
Agence canadienne de développement international	0	1	**1**
Agence des services frontaliers du Canada	1	28	**29**
Agence du revenu du Canada	1	52	**53**
Anciens Combattants Canada	3	12	**15**
Banque de développement du Canada	0	1	**1**
Bibliothèque et Archives Canada	0	2	**2**
Centre d'analyse des opérations et déclarations financières du Canada	1	2	**3**
Citoyenneté et Immigration Canada	0	16	**16**
Commissariat à l'information du Canada	0	4	**4**
Commissariat aux langues officielles	0	1	**1**
Commission canadienne des droits de la personne	1	3	**4**
Commission de l'immigration et du statut de réfugié	0	3	**3**
Commission de la fonction publique du Canada	0	1	**1**

PLAINTES REÇUES PAR INSTITUTION (suite)

Institution	Règlement rapide	Plaintes officielles	Total
Commission des relations de travail dans la fonction publique	1	1	**2**
Commission nationale des libérations conditionnelles	0	1	**1**
Conseil de la radiodiffusion et des télécommunications canadiennes	1	0	**1**
Conseil national de recherches Canada	0	1	**1**
Défense nationale	1	64	**65**
Diversification de l'économie de l'Ouest Canada	0	1	**1**
Environnement Canada	0	1	**1**
Finances Canada	0	1	**1**
Gendarmerie royale du Canada	12	63	**75**
Industrie Canada	0	1	**1**
Justice Canada	0	9	**9**
Parcs Canada	0	2	**2**
Passeport Canada	2	0	**2**
Pêches et Océans Canada	0	4	**4**
Ressources humaines et Développement des compétences Canada	5	20	**25**
Santé Canada	0	8	**8**
Secrétariat du Conseil du Trésor du Canada	4	1	**5**
Sécurité publique Canada	0	1	**1**
Service canadien du renseignement de sécurité	1	15	**16**
Service correctionnel du Canada	19	257	**276**
Service des poursuites pénales du Canada	0	1	**1**
Société canadienne des postes	9	18	**27**
Société Radio-Canada	1	1	**2**
Statistique Canada	2	2	**4**
Transports Canada	1	13	**14**
Travaux publics et Services gouvernementaux Canada	7	1	**8**
Tribunal canadien des droits de la personne	0	4	**4**
VIA Rail Canada	0	1	**1**
Total	**76**	**632**	**708**

PLAINTES REÇUES PAR PROVINCE OU TERRITOIRE

Province ou territoire	Plaintes	Règlement rapide	Total	Pourcentage
Ontario	192	21	**213**	30
Québec	173	19	**192**	27
Colombie-Britannique	142	20	**162**	23
Alberta	43	7	**50**	7
Terre-Neuve-et-Labrador	24	0	**24**	3
Manitoba	20	2	**22**	3
Saskatchewan	18	0	**18**	3
Nouvelle-Écosse	8	2	**10**	1
Nouveau-Brunswick	7	2	**9**	1
Île-du-Prince-Édouard	4	1	**5**	0,7
Nunavut	0	1	**1**	0,1
International*	1	1	**2**	0,2
Total	**632**	**76**	**708**	**100**

Le nombre de plaintes provenant du Québec a plus que doublé de 2009-2010 à 2010-2011, passant de 87 (13 % de toutes les plaintes) à 192, ou 27 % de toutes les plaintes au cours de l'exercice financier. Cette augmentation, attribuable en grande partie à de nombreuses plaintes formulées par un petit groupe de plaignants, a fait passer la province de la troisième à la deuxième place, devant la Colombie-Britannique.

* Les citoyens canadiens, les résidents permanents, les détenus des pénitenciers canadiens et les autres personnes « présentes au Canada » ont le droit d'accéder à leurs renseignements personnels. Ces personnes ont donc également le droit de déposer une plainte au Commissariat si elles se voient refuser l'accès à leurs renseignements personnels. Les Canadiennes et Canadiens vivant à l'étranger ont les mêmes droits en matière d'accès et de plainte que ceux qui vivent au Canada, et deux personnes ont choisi d'exercer ce droit en 2010-2011. Les dispositions des articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, qui portent entre autres sur la collecte, l'utilisation, la communication, la conservation et le retrait des renseignements personnels, visent toutes les personnes au sujet desquelles le gouvernement recueille des renseignements personnels, peu importe leur citoyenneté ou leur pays de résidence. Toute personne peut déposer une plainte au Commissariat à ce sujet.

DÉCISION PAR TYPE DE PLAINTE

Type de plainte		Conclusions			Autres issues			Total
		Fondée*	Non fondée	Résolue	Abandonnée	Réglée rapidement	Réglée en cours d'enquête	
Accès	Accès	32	108	13	20	26	6	**205**
	Correction/ annotation	1	0	0	0	3	0	**4**
	Frais	0	0	0	0	1	0	**1**
	Langue	2	0	0	0	0	0	**2**
Délais	Avis de prorogation	12	10	0	2	0	0	**24**
	Délais	208	13	0	6	6	0	**233**
Protection des renseignements personnels	Collecte	1	4	0	0	9	0	**14**
	Conservation et retrait	4	1	0	3	0	0	**8**
	Utilisation et communication	21	13	0	10	33	2	**79**
Total		**281**	**149**	**13**	**41**	**78**	**8**	**570**

Délais : Les plaintes au sujet du temps que prennent les institutions pour répondre aux demandes d'accès aux renseignements personnels étaient le type de plaintes que nous avons réglées le plus fréquemment l'an dernier : 257 plaintes au total, soit 45 % du nombre de cas. Puisque les plaignants s'adressent à nous une fois que le délai prescrit pour répondre à leur demande est effectivement échu, 220 de ces plaintes (86 %) étaient fondées.

Accès : Nous avons fermé au total 212 dossiers de plaintes concernant l'accès aux renseignements personnels, ce qui représente 37 % du nombre de dossiers clos au cours de l'exercice précédent. Plus du quart de ces dossiers ont été abandonnés, réglés rapidement ou réglés en cours d'enquête. Pour ce qui est des 156 cas restants, l'enquête n'a pas révélé que les plaintes étaient fondées dans 108 cas (69 %), tandis que 35 plaintes (22 %) ont été jugées fondées. Dans le cas de 13 dossiers relatifs à l'accès, l'enquête a

* Comprend 31 cas d'accès auparavant classés comme « fondés et résolus ».

permis de déterminer que la plainte était fondée. Mais ces cas ont été résolus au terme d'une négociation plutôt que par une conclusion officielle.

Protection des renseignements personnels : Les cas portant sur la collecte, l'utilisation, la communication, la conservation ou le retrait de renseignements personnels ont représenté 101 plaintes, soit 18 % du nombre de dossiers clos en 2010-2011. Nos enquêtes ont révélé que 26 plaintes étaient fondées et que 18 étaient non fondées. La grande majorité des plaintes relatives à la protection des renseignements personnels concernait l'utilisation ou la communication inappropriée de renseignements personnels.

DÉCISION À L'ÉGARD DES PLAINTES RELATIVES AUX DÉLAIS PAR INSTITUTION

	Fondée	Non fondée	Règlement rapide	Réglée en cours d'enquête	Abandonnée	Total
Affaires étrangères et Commerce international Canada	0	1	0	0	0	**1**
Agence canadienne d'inspection des aliments	4	2	1	0	0	**7**
Agence de la santé publique du Canada	1	0	0	0	0	**1**
Agence des services frontaliers du Canada	5	2	1	0	0	**8**
Agence du revenu du Canada	20	4	1	0	0	**25**
Citoyenneté et Immigration Canada	3	0	0	0	0	**3**
Commission canadienne des droits de la personne	0	0	1	0	0	**1**
Défense nationale	23	0	0	0	0	**23**
Gendarmerie royale du Canada	4	3	0	0	0	**7**
Justice Canada	2	2	0	0	0	**4**
Pêches et Océans Canada	0	1	0	0	0	**2**
Ressources humaines et Développement des compétences Canada	4	2	0	0	0	**6**
Santé Canada	3	1	0	0	0	**4**
Service canadien du renseignement de sécurité	1	0	0	0	0	**1**
Service correctionnel du Canada	141	5	2	0	4	**152**
Service des poursuites pénales du Canada	1	0	0	0	0	**1**
Société canadienne des postes	0	0	0	0	3	**3**
Transports Canada	8	0	0	0	0	**8**
Travaux publics et Services gouvernementaux Canada	0	0	0	0	1	**1**
Total	**220**	**23**	**6**	**0**	**8**	**257**

DÉCISION À L'ÉGARD DES PLAINTES RELATIVES À L'ACCÈS OU À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS PAR INSTITUTION

	Fondée*	Non fondée	Réglée	Réglée rapidement	Réglée en cours d'enquête	Abandonnée	Total
Affaires étrangères et Commerce international Canada	1	1	1	1	0	0	**4**
Affaires indiennes et du Nord Canada	1	0	0	1	1	1	**4**
Agence de la santé publique du Canada	0	0	0	1	0	1	**2**
Agence des services frontaliers du Canada	2	4	0	3	2	1	**12**
Agence du revenu du Canada	2	8	0	1	1	2	**14**
Agriculture et Agroalimentaire Canada	1	0	0	0	0	0	**1**
Anciens Combattants Canada	1	0	0	2	0	2	**5**
Bibliothèque et Archives Canada	0	0	0	0	0	1	**1**
Centre d'analyse des opérations et déclarations financières du Canada	0	0	0	1	0	0	**1**
Citoyenneté et Immigration Canada	2	0	1	1	1	1	**6**
Commissariat à l'information du Canada	0	1	0	0	0	0	**1**
Commissariat aux langues officielles	0	0	0	0	0	1	**1**
Commission canadienne des droits de la personne	1	0	0	1	0	0	**2**
Commission canadienne du blé	0	1	0	0	0	0	**1**
Commission de l'immigration et du statut de réfugié	0	1	0	0	0	0	**1**
Commission de la fonction publique	0	3	0	0	0	0	**3**
Commission nationale des libérations conditionnelles	1	0	1	0	0	0	**2**
Conseil de recherches en sciences humaines du Canada	1	0	0	0	0	0	**1**
Conseil national de recherches Canada	0	0	0	1	0	0	**1**
Défense nationale	8	22	0	2	1	4	**37**

DÉCISION À L'ÉGARD DES PLAINTES RELATIVES À L'ACCÈS OU À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS PAR INSTITUTION (suite)

	Fondée*	Non fondée	Réglée	Réglée rapidement	Réglée en cours d'enquête	Abandonnée	Total
Environnement Canada	0	0	1	0	0	0	**1**
Finances Canada	0	1	0	0	0	0	**1**
Gendarmerie royale du Canada	3	14	0	11	0	2	**30**
Industrie Canada	1	0	0	0	0	0	**1**
Justice Canada	1	2	0	0	0	0	**3**
Parcs Canada	0	1	0	0	0	0	**1**
Passeport Canada	0	0	0	2	0	0	**2**
Radio-Canada	2	0	0	1	0	0	**3**
Ressources humaines et Développement des compétences Canada	4	3	1	3	1	0	**12**
Santé Canada	2	0	0	0	0	2	**4**
Secrétariat du Conseil du Trésor du Canada	0	0	0	4	0	0	**4**
Sécurité publique Canada	0	0	1	0	0	0	**1**
Service canadien du renseignement de sécurité	0	7	0	1	0	0	**8**
Service correctionnel du Canada	14	47	4	15	1	10	**91**
Service des poursuites pénales du Canada	0	0	0	7	0	0	**7**
Société canadienne des postes	10	5	2	9	0	1	**27**
Statistique Canada	1	2	0	3	0	3	**9**
Transports Canada	1	2	1	1	0	1	**6**
Travaux publics et Services gouvernementaux Canada	1	1	0	0	0	0	**2**
Total	**61**	**126**	**13**	**72**	**8**	**33**	**313**

* Comprend 31 cas d'accès auparavant classés comme « fondés et résolus ».

DURÉE DE TRAITEMENT DES ENQUÊTES FAISANT SUITE À DES PLAINTES EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Dossiers de règlement rapide par type de plainte

Type de plainte	Dossiers	Délais de traitement moyens (en mois)
Utilisation et communication	33	3,1
Accès	26	3,4
Collecte	9	5,0
Délais	6	3,8
Correction/annotation	3	4,1
Frais	1	10,4
Total	**78**	**3,6**

Enquêtes officielles par type de plainte

Type de plainte	Dossiers	Délais de traitement moyens (en mois)
Délais	227	5,9
Accès	179	10,1
Utilisation et communication	46	9,9
Avis de prorogation	24	6,0
Conservation et retrait	8	12,6
Collecte	5	12,4
Langue	2	3,0
Correction/annotation	1	14,0
Total	**492**	**8,0**

Tous les dossiers réglés par décision

Type de plainte	Dossiers	Délais de traitement moyens (en mois)
Fondée	250	6,8
Non fondée	149	8,6
Réglée rapidement	78	3.6
Abandonnée	41	7,6
Fondée et résolue	31	13,4
Résolue	13	9,2
Réglée en cours d'enquête	8	11,0
Total	**570**	**7,2**

La durée de traitement est mesurée à partir de la date où la plainte est reçue jusqu'à la date à laquelle l'enquête se termine, que ce soit par la formulation de constatations ou par un autre moyen.

L'importance que nous accordons aux stratégies de règlement rapide nous a permis de réduire les délais de traitement moyens, qui sont passés de 19,5 mois en 2008-2009 à 12,9 mois en 2009-2010 et à 7,2 mois en 2010-2011.