Commissariat
à la protection de
la vie privée du Canada

Vie privée

Rapport annuel au Parlement
2010

Rapport sur la
Loi sur la protection des renseignements
personnels et les documents électroniques

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

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

N° de catalogue IP51-1/2010F-PDF
ISBN : 978-1-100-96576-5

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) 995-8210
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) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Juin 2011

L'honorable Noël A. Kinsella, sénateur
Président
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Monsieur,

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 et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2010.

Veuillez agréer, Monsieur, 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) 995-8210
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) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Juin 2011

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

Monsieur,

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 et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2010.

Veuillez agréer, Monsieur, 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

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) établit des règles de base à l'égard de la gestion des renseignements personnels dans le secteur privé.

Elle vise l'atteinte d'un équilibre entre le droit à la protection des renseignements personnels et le besoin qu'ont les organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins commerciales légitimes.

La LPRPDE s'applique aux organisations qui se livrent à des activités commerciales à la grandeur du pays, sauf celles qui sont régies par des provinces disposant de leur propre législation sur la protection des renseignements personnels pour le secteur privé. Le Québec, l'Alberta et la Colombie-Britannique disposent de leur propre loi applicable au secteur privé. Toutefois, même dans ces provinces, le LPRPDE s'applique au secteur privé assujetti à la réglementation fédérale et aux renseignements personnels dans le cadre de transactions interprovinciales et internationales. Les provinces de l'Atlantique, l'Ontario, le Manitoba, le Saskatchewan et les territoires sont visés par la LPRPDE.

La LPRPDE protège également les renseignements des employés travaillant dans les secteurs régis par la réglementation fédérale.

Message de la commissaire

À l'ère numérique, la protection du droit à la vie privée s'avère un défi de plus en plus complexe. Une partie toujours plus importante de notre vie quotidienne se déroule sur Internet et nos activités peuvent être facilement surveillées, mises en mémoire, analysées et des renseignements sur celles-ci peuvent être communiqués.

Les enjeux complexes de la protection de la vie privée dans le monde numérique ont occupé une place prépondérante dans le cadre de nos travaux en 2010.

Vu le déplacement de notre vie sociale vers le monde virtuel, les mesures de protection de la vie privée sont devenues essentielles. Nous avons eu le plaisir de faire part, en septembre, de notre satisfaction à l'égard des améliorations à la protection de la vie privée qu'a apportées Facebook sur son site, en réaction aux conclusions de notre enquête exhaustive.

Par ailleurs, notre enquête sur la collecte par Google de données de nature délicate transmises par des réseaux sans fil non sécurisés a révélé les déficiences des mesures de contrôle de la protection de la vie privée.

Compte tenu de la dimension complexe et changeante de cet environnement et de la tendance à l'exhibitionnisme numérique, on évoque de plus en plus l'éventuelle disparition du concept de vie privée.

Bien sûr, la perception de ce que devrait constituer la protection de la vie privée évolue au fil du temps et d'une génération à l'autre. Cependant, il me semble évident que le respect de la vie privée continue d'être une valeur primordiale – et nous en avons eu de nombreuses preuves en 2010.

UNE « NOUVELLE NORME SOCIALE »

Au début de l'année, Mark Zuckerberg, chef de la direction de Facebook, a livré son opinion sur la protection de la vie privée :

> *Les gens sont de plus en plus à l'aise non seulement d'échanger de l'information de toute sorte, mais aussi de le faire de plus en plus ouvertement et avec un nombre croissant de personnes. Cette norme sociale a simplement évolué avec le temps. Nous croyons qu'il est de notre rôle […] d'innover constamment et de faire en sorte que notre système reflète les normes sociales actuelles.* [traduction]

Je suis d'accord avec l'observation selon laquelle les normes sociales auraient évolué. La vie privée a changé depuis une génération, même depuis la dernière décennie. Il est surprenant de voir comment certaines personnes affichent sans fard leur vie privée en ligne.

Mais je me réjouis également de tous les signes montrant que le public est constamment préoccupé par le respect de la vie privée, une préoccupation que partagent les jeunes, qui sont les plus grands utilisateurs d'Internet.

Nous le constatons lorsque nous visitons les écoles pour parler aux enfants et aux adolescents de la 4e à la 12e année de la gestion de leur réputation en ligne. À la fin de chaque présentation, les jeunes posent des questions qui révèlent à quel point ils s'intéressent à la protection de la vie privée. Ils veulent savoir comment contrôler les données de leur profil en ligne et savoir ce qui est vu et par qui. Ils veulent savoir comment s'y prendre pour être mis au courant de tout ce que les autres utilisateurs affichent à leur sujet. Et ils demandent souvent comment supprimer définitivement de l'information – que ce soit du matériel qu'ils souhaiteraient ne pas avoir affiché ou des réponses à de vieux jeux-questionnaires qu'ils ne veulent plus voir apparaître sur Internet.

Le droit à la vie privée demeure une valeur extrêmement importante et chère aux yeux des Canadiennes et des Canadiens, et des citoyens du monde entier.

Ceux qui essaient de nous convaincre que le concept de vie privée est démodé sont généralement ceux qui tentent de tirer profit de sa disparition.

Les renseignements personnels sont devenus un bien précieux et un moyen de s'enrichir pour certaines entreprises. Il n'est donc pas étonnant que certaines d'entre elles veulent banaliser l'importance de la vie privée.

J'ai même entendu la question suivante : « La vie privée et l'innovation peuvent-elles coexister? »

Il est indéniable que la protection de la vie privée n'entrave pas l'innovation.

La pression exercée sur la vie privée n'est pas liée uniquement aux nouvelles normes sociales ou aux nouvelles technologies. Dans le secteur commercial auquel s'applique

la LPRPDE, elle provient en premier lieu du fait qu'il peut s'avérer très lucratif de repousser les limites de la vie privée.

RÉACTIONS

Toutefois, les gens font preuve de résistance.

Nous en avons été témoins lors des remous causés par deux géants du monde virtuel : Facebook et Google.

Les utilisateurs de Facebook ont réagi avec force quand le site de réseautage social a mis en œuvre une série de modifications qui rendaient beaucoup plus difficile pour les utilisateurs de protéger leur vie privée. Les protestations ont porté fruit et ont forcé Facebook à annuler certaines de ces modifications.

De son côté, Google a lui aussi déclenché un tollé lors du lancement de Google Buzz au début de 2010.

Du jour au lendemain, l'entreprise a combiné Gmail, un service de courriel Web privé, à son nouveau service de réseautage social. Google a automatiquement assigné à ses utilisateurs un réseau « d'amis » formé des personnes avec qui ils correspondaient le plus sur Gmail. Google a entrepris ces démarches sans informer adéquatement les utilisateurs au sujet du fonctionnement de ce nouveau service ni leur fournir suffisamment de renseignements pour que ceux-ci soient en mesure de donner un consentement éclairé.

Cette opération a soulevé une tempête de protestations chez les utilisateurs partout dans le monde qui craignaient, à juste titre, que leurs renseignements personnels soient communiqués.

Le lancement d'un produit présentant de telles failles en matière de protection de la vie privée témoignait d'un mépris désolant envers les normes et les lois fondamentales régissant ce domaine. Je faisais partie du groupe des dix autorités internationales de protection des données qui ont envoyé une lettre conjointe à Google pour lui rappeler la nécessité de respecter les lois en vigueur dans les pays où elle commercialise ses produits. Cette initiative constitue une autre preuve de l'engagement à l'égard du droit à la vie privée qui a cours à l'échelle internationale.

Il faut cependant reconnaître que Google s'est rapidement excusé et a apporté des modifications pour désamorcer les critiques.

LA VIE PRIVÉE DEMEURE UNE VALEUR IMPORTANTE

Ces deux exemples illustrent l'importance que les gens accordent encore à la protection de leur vie privée.

Oui, de nombreuses personnes, surtout les jeunes, acceptent de communiquer davantage de renseignements personnels que ne le consentaient les générations précédentes, mais elles veulent le faire à leur manière. Elles veulent exercer un contrôle sur leurs renseignements personnels. Cette aspiration constitue justement un des fondements de la législation sur la protection de la vie privée au Canada et dans un grand nombre d'autres pays.

Il est clair que les Canadiennes et les Canadiens apprécient bon nombre des nouveaux services qui sont offerts en ligne et qu'ils veulent continuer à les utiliser pour communiquer entre eux. Plus de la moitié de la population canadienne est maintenant sur Facebook.

Mais il est également évident que les utilisateurs veulent des services qui respectent leur vie privée. C'est ce que les Canadiennes et les Canadiens ont affirmé dans les courriels et les lettres qu'ils ont fait parvenir au Commissariat, et c'est ce que j'entends quand je voyage au pays.

J'ai le sentiment très net que nous parlons *vraiment* au nom de la population canadienne lorsque nous demandons à ces grandes entreprises en ligne de respecter nos lois.

LA PROTECTION DE LA VIE PRIVÉE EN LIGNE

La protection de la vie privée en ligne revêt une importance sans cesse grandissante pour le Commissariat, et c'est pourquoi nous avons décidé d'en faire un thème majeur du rapport annuel de cette année.

Il est indéniable que ce domaine offre de multiples défis. Les enjeux sont souvent complexes et très techniques. Les sites Web évoluent quotidiennement; demeurer à jour exige donc beaucoup de travail. L'environnement en ligne auquel les Canadiennes et les Canadiens accèdent pour se procurer des produits et des services est mondial. Bien souvent, les organisations avec lesquelles nous faisons affaire sont établies à l'étranger.

Il ne fait aucun doute que le monde numérique pose des défis de taille pour le droit à la vie privée. Cela veut dire que nous devons travailler plus fort et de façon plus intelligente, et non pas jeter l'éponge et « en revenir » – conformément à cette citation célèbre d'un géant de la technologie.

Nous *pouvons* agir de multiples façons devant les nouveaux risques pour la vie privée qui découlent des changements technologiques :

- Nous devons appliquer nos lois sur la protection de la vie privée et nous assurer qu'elles demeurent actuelles et pertinentes.

- Nous devons renforcer la collaboration entre les autorités chargées de protéger la vie privée, car nous sommes bien plus forts lorsque nous nous exprimons d'une seule voix.

- En tant que société, nous devons nous assurer de combler l'écart existant entre nos connaissances en matière de protection de la vie privée et notre connaissance du monde en ligne.

DES LOIS ADAPTÉES AUX NOUVELLES RÉALITÉS

Les technologies évoluent à un rythme stupéfiant, et ces changements soulèvent de nouvelles questions intéressantes du point de vue juridique.

Est-ce que les lois conçues pour le monde réel peuvent protéger la vie privée en ligne? Devons-nous adopter de nouvelles lois? Comment traiter les cas relatifs aux juridictions et à l'application de la loi lorsque des entreprises internationales en ligne sont en cause?

De toute évidence, le cadre réglementaire protégeant le droit des Canadiennes et des Canadiens à la vie privée est mis à l'épreuve étant donné l'évolution rapide des technologies.

Il est essentiel que nous nous assurions de toujours actualiser nos lois pour être en mesure de relever les défis actuels et futurs.

Les artisans de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ont fait preuve de prévoyance en rédigeant une loi qui demeure neutre sur le plan de la technologie et qui doit faire l'objet d'un examen parlementaire tous les cinq ans.

Le premier examen a débuté à la fin de 2006, et le deuxième devrait être amorcé en 2011.

Le Commissariat a déjà entamé le travail préparatoire en vue du prochain examen.

Nous avons commandé un rapport sur l'efficacité de notre modèle d'ombudsman actuel. Nous avons en outre tenu des consultations publiques sur le suivi, le profilage et le ciblage en ligne des consommateurs effectués par les spécialistes du marketing ou d'autres entreprises, et sur l'infonuagique.

Le rapport, de même que nos consultations publiques, nous aideront à préparer notre intervention dans le cadre du prochain examen parlementaire de la LPRPDE.

Le rapport a été préparé par deux universitaires reconnus : Lorne Sossin, doyen de la Osgoode Hall Law School, et France Houle, professeure de droit à l'Université de Montréal. Nous leur avons demandé d'examiner l'efficacité du modèle d'ombudsman pour la protection des renseignements personnels dans le secteur privé, particulièrement à la lumière des changements qui se sont opérés sur les plans technologique, économique et juridique depuis l'entrée en vigueur de la LPRPDE.

À la suite de leur analyse, les auteurs du rapport démontrent que le modèle actuel d'ombudsman a eu un succès mitigé.

Sur une note positive, les auteurs estiment que le Commissariat a su atteindre des objectifs majeurs en matière de conformité en collaborant avec de grands secteurs de l'industrie comme les banques et les assurances, en gagnant la confiance du secteur privé, en facilitant l'interprétation et l'application de la LPRPDE, en donnant suite aux plaintes, aux demandes de renseignements et aux préoccupations, en exposant la pertinence de la LPRPDE et en rehaussant de manière générale la visibilité des enjeux liés à la protection de la vie privée.

Les auteurs sont toutefois d'avis que le modèle d'ombudsman est d'une efficacité moindre lorsqu'il est question de veiller à la conformité en ce qui a trait aux petites et aux moyennes entreprises.

Ainsi, ils proposent comme solution d'octroyer au Commissariat le pouvoir précis et limité de rendre des ordonnances, y compris d'imposer des sanctions telles que des amendes. Ils recommandent également l'ajout du pouvoir explicite d'élaborer des directives en appui à la mise en place équitable et transparente des nouveaux pouvoirs exécutoires.

Le Commissariat procède présentement à l'évaluation de cette analyse, et ce en appliquant celle-ci à son expérience liée à la LPRPDE et en la comparant à sa propre appréciation des avantages et de l'efficacité du modèle d'ombudsman. Cette étude alimentera de façon substantielle le discours public sur l'évolution de cette loi.

Par ailleurs, nos consultations publiques nous ont permis de mieux comprendre quelques-unes des nouvelles tendances en matière de technologies qui auront des répercussions importantes sur la vie privée des Canadiennes et des Canadiens.

Ces consultations étaient une première pour nous. Nous avons sollicité des observations écrites, mais nous avons aussi tenu des discussions de groupe d'une journée à Toronto, à Montréal et à Calgary, ce qui nous a permis de recueillir un large éventail de points

de vue provenant des entreprises, des administrations gouvernementales, du milieu universitaire, des associations de consommateurs et du public en général.

Au moment de la préparation du présent rapport annuel, nous finalisions le rapport final sur les consultations qui sera publié en 2011.

Alors que nous commençons à réfléchir aux recommandations pour la réforme de la LPRPDE dans le cadre du prochain examen parlementaire, nous entrevoyons également les modifications qui découlent du dernier examen.

Elles prennent la forme de deux projets de loi – l'un d'eux a reçu la sanction royale en décembre 2010 et l'autre était encore devant le Parlement au début de 2011.

Le projet de loi encore à l'étude au Parlement modifierait la LPRPDE pour, entre autres choses, obliger les organisations à informer le Commissariat et les personnes touchées en cas de graves atteintes à la protection des données. Un tel changement serait providentiel.

Le projet de loi qui a été adopté vise à endiguer le volume de communications électroniques néfastes et trompeuses (pourriels) qui circulent au Canada. Dans l'année qui vient, nous comptons assumer les responsabilités en matière d'application de la loi qui nous incombent en vertu de la nouvelle loi sur l'élimination des pourriels.

Cette loi modifie la LPRPDE pour conférer au Commissariat un plus grand pouvoir discrétionnaire quant au rejet ou à l'abandon de plaintes, et lui permettre de partager des informations avec ses homologues à l'échelle nationale ou internationale, que l'affaire porte sur les pourriels ou sur d'autres enjeux liés au respect de la vie privée. De manière générale, ces deux pouvoirs discrétionnaires s'appliquent aux enquêtes.

COLLABORATION ACCRUE

Nous devons également travailler au-delà de nos frontières. Le Canada ne peut s'attaquer seul à toutes les inquiétudes soulevées par le Web relativement au respect de la vie privée.

Il s'est passé beaucoup de choses sur la scène mondiale. Nous participons, par exemple, à plusieurs initiatives visant à élaborer une norme internationale en matière de protection de la vie privée, et nous sommes un membre fondateur du nouveau Global Privacy Enforcement Network (réseau mondial d'exécution des lois sur la protection des renseignements personnels).

Nous apportons par ailleurs notre concours aux activités de protection de la vie privée de la Coopération économique Asie-Pacifique (APEC) et de l'Organisation de coopération

et de développement économiques (OCDE), qui fêtait en 2010 le 30e anniversaire de ses *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*.

L'année 2010 a vu la collaboration sans précédent du Commissariat et de neuf homologues de la scène internationale, qui ont fait front commun pour rappeler à Google et à d'autres entreprises en ligne la responsabilité qu'il leur incombe de respecter les lois sur la protection des renseignements personnels partout dans le monde dans le cadre de lancements de nouveaux produits et services.

Toutes les autorités qui ont participé à ce projet ont reconnu la nécessité de s'unir, autant que possible, pour que leur message soit entendu.

CONNAISSANCES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Un autre aspect important de la protection de la vie privée en ligne consiste à trouver des façons de mieux faire comprendre aux consommateurs et aux organisations les enjeux liés à la protection de la vie privée.

La population canadienne est réputée adopter rapidement les nouvelles technologies. En effet, 80 % des Canadiennes et des Canadiens de plus de 16 ans utilisent maintenant le Web. Si nous possédons des connaissances approfondies en matière de technologies, nous aurions avantage à poursuivre notre éducation sur la protection de la vie privée dans le contexte du monde numérique.

Un grand nombre d'utilisateurs ne savent pas qu'ils laissent des traces numériques quand ils naviguent sur le Web et ignorent que ces informations sont stockées, analysées, rendues disponibles et qu'elles sont susceptibles d'être utilisées d'une manière qu'ils n'avaient pas prévue.

Combien de personnes lisent vraiment les politiques sur la protection des renseignements personnels? Les gens savent-ils comment sécuriser leurs ordinateurs et leurs réseaux à domicile?

La nécessité d'améliorer les connaissances en matière de protection de la vie privée s'applique non seulement aux personnes, mais aussi aux organisations. Les entreprises doivent s'assurer que leurs employés sont compétents en la matière, et qu'ils connaissent la façon d'utiliser et de traiter les renseignements personnels conformément aux valeurs relatives à la protection de la vie privée.

Nous sommes d'ardents partisans de ce type de formation, qui peut permettre à une organisation d'éviter bien des ennuis et de dépenses inutiles. Un employé qui a eu la

possibilité d'approfondir ses connaissances en matière de protection de la vie privée est moins susceptible de laisser un ordinateur portatif contenant des renseignements personnels sur le siège avant de sa voiture et fait preuve de vigilance en composant un numéro de télécopieur pour transmettre des documents de nature délicate.

La formation – celle qui est *continue* – incite les gens à prendre le temps de réfléchir à la nécessité de protéger les renseignements personnels. Elle les sensibilise au fait que les renseignements personnels devraient être privés a priori.

Un sondage récent effectué pour le Commissariat a révélé que seulement 37 % des entreprises avaient offert une formation sur la protection de la vie privée à leurs employés. Il faut faire mieux.

BUREAU DE TORONTO

Un jalon important dans l'histoire du Commissariat à la protection de la vie privée du Canada a été posé en 2010. En effet, nous avons ouvert notre premier bureau à l'extérieur de la capitale nationale.

Le nouveau Bureau de Toronto nous permettra d'être plus présents dans le cadre d'activités de sensibilisation et des enquêtes relatives à la LPRPDE. Un très grand pourcentage des plaintes déposées contre des organisations du secteur privé visent des entreprises établies dans la région du Grand Toronto.

Nous nous attendons à ce que le Bureau de Toronto ouvre la voie à des relations plus solides et plus efficaces avec nos intervenants de la métropole, ce qui, au bout du compte, entraînera une meilleure protection de la vie privée des Canadiennes et des Canadiens.

NOUVEAU MANDAT

À la fin de 2010, j'ai eu l'honneur de voir mon mandat à titre de commissaire à la protection de la vie privée du Canada reconduit.

Ce fut un grand privilège de servir la population canadienne et le Parlement au cours des sept dernières années, et j'apprécie grandement la confiance que me témoignent encore une fois le premier ministre et le Parlement. Le Commissariat pourra ainsi continuer à bâtir à partir de nos assises et poursuivre les projets en cours.

J'ai été touchée par les éloges que le Commissariat a reçus pour le travail accompli ces dernières années. Bien que j'aimerais apporter des améliorations pour m'assurer que nous servons le mieux possible les Canadiennes et les Canadiens, nous comptons plusieurs réalisations dont nous pouvons être fiers.

Le secret de ces réussites réside dans l'équipe professionnelle et dévouée œuvrant au Commissariat à la protection de la vie privée du Canada, un groupe de personnes réfléchies, créatives, passionnées, déterminées et infatigables qui sont toujours prêtes à relever les défis posés par les enjeux toujours plus complexes relatifs à la protection de la vie privée.

Les effectifs du Commissariat ont augmenté ces dernières années, et nous avons eu la chance de recruter des personnes extraordinairement talentueuses et hautement compétentes.

Ce rapport annuel me fournit l'occasion d'exprimer à tout le personnel du Commissariat ma vive gratitude pour son travail remarquable, qui a des répercussions très positives sur la vie quotidienne de la population canadienne.

Au milieu de l'année 2010, Elizabeth Denham, la commissaire adjointe chargée de la LPRPDE, a été nommée commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique. Même si elle nous manquera à Ottawa, comme amie et comme collègue, nous sommes ravis de pouvoir compter dorénavant sur une autre alliée en Colombie-Britannique et d'avoir la chance de continuer à travailler avec elle sur des dossiers communs.

À la suite de cette nomination, les responsabilités de la commissaire adjointe Chantal Bernier ont été élargies. Elle est maintenant responsable de la *Loi sur la protection des renseignements personnels* – la loi sur la protection de la vie privée applicable au gouvernement fédéral – et de la LPRPDE. Je lui suis reconnaissante d'avoir accepté un défi aussi énorme, et je veux lui exprimer ma profonde gratitude pour son dévouement indéfectible et son leadership exceptionnel au sein du Commissariat.

Au cours des trois prochaines années, notre équipe aura l'occasion de s'attaquer à de nombreuses questions, qu'elles soient nouvelles ou déjà existantes, liées à la protection de la vie privée. Il nous reste encore de nombreux défis à relever, notamment l'amélioration de la prestation de services aux Canadiennes et aux Canadiens qui communiquent avec le Commissariat pour obtenir de l'aide.

Dans un contexte qui évolue rapidement, la protection de la vie privée exige des solutions astucieuses et créatives. C'est ce que nous nous emploierons à faire au nom des Canadiennes et des Canadiens.

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

La protection de la vie privée en chiffres

LE COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA EN 2010

Demandes de renseignements reçues liées à la LPRPDE	4 793
Plaintes reçues pour règlement rapide liées à la LPRPDE	108
Plaintes reçues liées à la LPRPDE	99
Enquêtes terminées liées à la LPRPDE	249
Lois et projets de loi soulevant des questions relatives à la LPRPDE examinés sous l'angle de leurs effets sur la protection de la vie privée	13
Politiques et initiatives du secteur privé examinées (Par exemple, une analyse concernant une nouvelle application technologique ou un article sur une pratique de l'industrie visant à tenir les membres du personnel au courant des nouveaux développements.)	30
Documents d'orientation stratégique publiés	14
Rapports de recherche publiés	5
Comparutions devant des comités parlementaires	13
Autres activités menées auprès de parlementaires ou de leur personnel (Par exemple, des réunions avec des députés ou des sénateurs.)	40
Discours prononcés et présentations	150
Ententes de contributions signées	16
Consultations du site Web principal du Commissariat Consultations des blogues et autres sites Web du Commissariat (dont le blogue du CPVP, le blogue des jeunes, le site Web des jeunes, le site de l'inspection approfondie des paquets et la chaîne YouTube) Total	2 349 741 1 124 258 3 473 999
« Tweets » envoyés	700
Publications distribuées	15 478
Entrevues accordées aux médias	250
Communiqués	42

Nota : Sauf indication contraire, ces données comprennent également les activités menées en vertu de la *Loi sur la protection des renseignements personnels*, qui sont décrites dans un rapport annuel distinct.

CHAPITRE 1

Le domaine de la protection de la vie privée

Principales réalisations en 2010

1.1 Prestation de services à la population canadienne

DEMANDES DE RENSEIGNEMENTS DU PUBLIC

En 2010, les Canadiennes et les Canadiens ont communiqué avec le Commissariat 9 200 fois, soit par téléphone soit par courrier postal. Environ la moitié de ces consultations portaient sur des enjeux relatifs à la protection de la vie privée dans le secteur privé visés par la LPRDPE. Les autres demandes de renseignements concernaient la *Loi sur la protection des renseignements personnels* ou portaient sur une question ne renvoyant pas exclusivement à l'une ou l'autre des lois dont nous surveillons l'application.

Du côté de la LPRDPE, nous avons constaté que le nombre de demandes de renseignements concernant le cyberespace avait continué d'augmenter.

Pour obtenir de plus amples renseignements sur ce sujet, veuillez consulter la rubrique 4.1.

PLAINTES DU PUBLIC

Grâce, en grande partie, aux efforts accrus que nous avons déployés pour régler les problèmes en amont, le nombre de plaintes officielles adressées au Commissariat a considérablement diminué en 2010.

Nous avons reçu 108 plaintes ayant mené à un règlement rapide et 99 nouvelles plaintes nécessitant une enquête officielle concernant le secteur privé. Le nombre total des plaintes s'élève donc à 207 comparativement à 231 en 2009.

Comme nous l'expliquons dans le chapitre 4, nos efforts investis pour aider les personnes et les organisations à régler leurs problèmes avant que ceux-ci ne donnent lieu à des plaintes officielles ont donné d'excellents résultats.

Nous avons notamment mis en place un système de règlement rapide, qui est vite devenu un instrument important pour régler les problèmes en temps opportun. Dans certains cas, un enjeu qui aurait pris des mois à régler par l'entremise du processus d'enquête officiel, peut maintenant être traité en quelques jours.

Dans la plupart des cas de règlement rapide, nous avons réussi à obtenir une solution satisfaisante sans recourir à une enquête officielle.

ENQUÊTES SUR LES PLAINTES

Nous avons résolu 249 plaintes visant le secteur privé en 2010.

Le cyberespace continue à occuper une grande place dans nos enquêtes. En 2010, nous nous sommes penchés sur des affaires mettant en cause d'importants joueurs du monde en ligne, tels que Facebook et Google. Nous avons également fait enquête sur le populaire site de rencontres eHarmony.

Le rapport de cette année porte surtout sur ces enjeux liés au cyberespace. On peut trouver des résumés de nos enquêtes à ce sujet au chapitre 2.

Des renseignements sur nos autres enquêtes sont fournis au chapitre 4.

SENSIBILISATION DU PUBLIC

Au cours de l'année 2010, la commissaire, les commissaires adjointes et d'autres représentants du Commissariat ont prononcé 150 discours et exposés, qui portaient dans plusieurs cas sur la protection de la vie privée dans le secteur privé.

On nous a également demandé de commenter des dizaines de reportages, dont un grand nombre traitaient de la protection de la vie privée dans le monde virtuel.

Nos publications ont continué de susciter l'intérêt : nous avons distribué 15 478 exemplaires de nos brochures, dépliants et guides à l'occasion de conférences et à la demande d'organisations et de particuliers.

En outre, le nombre de consultations de notre site Web a augmenté de 36 % par rapport à l'année précédente.

Nous continuons de nous intéresser de près à la protection de la vie privée des enfants et des adolescents en ligne par le truchement de la création de sites Web pour les jeunes et d'un populaire programme de présentations dans les écoles. En 2010, nous avons également donné notre appui au premier PrivacyCampTO annuel, une conférence sur la protection de la vie privée à l'ère numérique.

Pour plus de renseignements sur nos initiatives de sensibilisation du public, veuillez vous reporter au chapitre 5.

1.2 Appui au Parlement

COMPARUTIONS DEVANT DES DÉPUTÉS ET DES SÉNATEURS

Au cours de l'année 2010, la commissaire, les commissaires adjointes et d'autres représentants du Commissariat ont comparu officiellement à 13 reprises devant des comités parlementaires.

En octobre, par exemple, nous avons comparu devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes dans le cadre de son examen des répercussions des applications d'imagerie à l'échelle de la rue sur la protection de la vie privée.

Les voitures-caméras de Google Street View avaient recueilli des données utiles de réseaux sans fil non protégés. Nous avons mis en place notre propre enquête à ce sujet.

Nous sommes heureux que le Comité se soit intéressé aux pratiques de Google en matière de traitement des renseignements personnels et à la protection de la vie privée des Canadiennes et des Canadiens. Dans notre témoignage, nous avons rappelé une fois de plus qu'il est indispensable de veiller à ce que la protection de la vie privée reste pour les entreprises un facteur clé dans l'élaboration de nouveaux produits et services nécessitant l'usage de renseignements personnels.

En janvier 2011, le Comité a déposé son rapport et s'est dit convaincu que les préoccupations des Canadiennes et des Canadiens concernant la technologie de l'imagerie à l'échelle de la rue étaient prises au sérieux par toutes les parties en cause.

Le Comité s'est montré rassuré à l'égard de la surveillance qu'exerce le Commissariat au fil de l'évolution de la situation quant à l'application de la loi canadienne sur la protection de la vie privée, ajoutant qu'il continuerait lui-même de suivre la question et qu'il y reviendrait au besoin.

Dans son rapport, le Comité a estimé que « les concepteurs de technologies doivent accorder une attention très particulière à la protection de la vie privée à l'étape de l'élaboration de leurs nouveaux projets. Il leur faut cerner les risques éventuels pour la vie privée et les supprimer ou les réduire dès le début des nouveaux projets, au lieu de les affronter après coup à grands frais ».

La question de la sécurité nationale — qui se pose parfois dans un contexte où le secteur privé joue un rôle — a continué de faire l'objet d'un dialogue entre le Commissariat et les comités parlementaires.

Par exemple, en novembre, nous avons comparu devant le Comité permanent des transports, de l'infrastructure et des collectivités de la Chambre des communes au sujet du projet de loi C-42, la *Loi modifiant la Loi sur l'aéronautique*. Le projet de loi – découlant des exigences du programme américain de sécurité aérienne (Secure Flight) – permettrait le partage de renseignements personnels entre les compagnies aériennes canadiennes et les autorités américaines lorsqu'un avion survole, sans s'y poser, le territoire des États-Unis.

Nous comprenons bien que la souveraineté des États-Unis englobe son espace aérien, mais nous avons estimé qu'il était important d'exprimer nos inquiétudes au sujet des conséquences éventuelles de ce programme sur la protection de la vie privée des voyageurs canadiens.

Dans notre témoignage, nous avons rappelé que le gouvernement du Canada a un rôle important à jouer en collaboration avec le gouvernement des États-Unis et les compagnies aériennes canadiennes pour réduire l'incidence de Secure Flight. Nous avons proposé que le gouvernement garantisse que ne soit communiqué que le minimum de renseignements personnels, qu'il conteste les périodes de conservation de l'information et qu'il négocie des mécanismes de recours solides et accessibles.

Nous avons également fait part de notre position dans le cadre d'autres audiences de comité, notamment les suivantes :

- L'audience du Comité sénatorial permanent des affaires sociales, des sciences et de la technologie concernant le projet de loi C-36, la *Loi concernant la sécurité des produits de consommation* – 25 novembre 2010.

- L'audience du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes concernant le rapport annuel au Parlement 2009-2010 sur la LPRPDE et le rapport annuel au Parlement 2009-2010 sur la *Loi sur la protection des renseignements personnels* – 19 octobre 2010.

- L'audience du Comité des transports, de l'infrastructure et des collectivités de la Chambre des communes concernant la sécurité aérienne – 11 mai 2010.

Au cours de l'année, nous avons également eu des échanges moins formels avec des parlementaires, notamment dans le cadre du suivi de nos comparutions devant les comités, d'examens de sujets particuliers avec des députés, de téléconférences, de réunions en personne et de séances d'information.

EXAMEN DES LOIS ET PROJETS DE LOI SUSCEPTIBLES D'AVOIR DES RÉPERCUSSIONS SUR LA VIE PRIVÉE

Nous avons examiné 27 projets de loi pour en vérifier les répercussions sur la vie privée. Environ la moitié de ces textes législatifs renvoyaient à des enjeux liés au secteur privé.

Il s'agissait des projets de loi suivants :

- C-22 — *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*.

- C-28 — *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes*, *la Loi sur la concurrence*, la *Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*.

- C-29 — *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques (Loi protégeant les renseignements personnels des Canadiens)*.

- C-32 — *Loi modifiant la Loi sur le droit d'auteur (Loi sur la modernisation du droit d'auteur)*.

- C-36 – *Loi concernant la sécurité des produits de consommation (Loi canadienne sur la sécurité des produits de consommation)*.

- C-42 — *Loi modifiant la Loi sur l'aéronautique (Loi sur le renforcement de la sûreté aérienne).*

- C-50 — *Loi modifiant le Code criminel (interception de communications privées et mandats et ordonnances connexes) (Loi visant à améliorer l'accès aux outils d'enquête sur les crimes graves)* .

- C-51 — *Loi modifiant le Code criminel, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle (Loi sur les pouvoirs d'enquête au 21e siècle)*

- C-52 — *Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes (Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention).*

RENOUVELLEMENT LÉGISLATIF

Dans un environnement où les enjeux relatifs à la protection de la vie privée évoluent constamment en raison des nouvelles technologies, il est indispensable de veiller à ce que la LPRPDE soit en mesure de protéger le droit des Canadiennes et Canadiens à la vie privée.

Heureusement, la LPRPDE (contrairement à la *Loi sur la protection des renseignements personnels*) doit être soumise à un examen parlementaire tous les cinq ans.

À la suite du premier examen, un certain nombre de modifications, s'inscrivant dans le cadre de deux projets de loi distinct, ont été apportées.

L'un de ces textes législatifs – un projet de loi visant à lutter contre les pourriels – a reçu la sanction royale à la fin de 2010 et donnera lieu à d'importants changements au Commissariat.

L'objet de cette mesure législative est d'éliminer les pourriels les plus nocifs ou frauduleux, de débarrasser le Canada des polluposteurs et de mettre fin aux attaques continuelles venant de l'extérieur du pays. Le Commissariat aura un rôle à jouer dans l'exécution de la loi, de concert avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau fédéral de la concurrence.

Grâce à ces modifications, le Commissariat pourra partager plus facilement de l'information avec ses homologues provinciaux et internationaux.

Cette mesure législative modifie également la LPRPDE pour conférer au commissaire à la protection de la vie privée le pouvoir discrétionnaire de rejeter ou d'abandonner des

plaintes. Cette modification, qui arrive en temps opportun, nous aidera à faire converger nos ressources limitées vers les enjeux les plus stratégiques pour les Canadiennes et les Canadiens.

Aux termes de ces modifications, nous pouvons rejeter une plainte dans l'un des cas suivants : le plaignant n'a pas épuisé les recours internes ou les procédures d'appel ou de règlement des griefs; la plainte pourrait avantageusement être traitée en vertu d'autres lois fédérales ou provinciales; le plaignant n'a pas déposé sa plainte dans un délai raisonnable.

En vertu d'autres modifications, le Commissariat se voit conférer le pouvoir discrétionnaire de mettre fin à des enquêtes, dans les cas suivants : les preuves sont insuffisantes, la plainte est frivole ou entachée de mauvaise foi, l'organisation a fourni une réponse valable; l'affaire fait déjà ou a fait l'objet d'une enquête.

S'il décide de rejeter ou d'abandonner la plainte, le Commissariat est tenu de fournir au plaignant et à l'organisation intimée les motifs de sa décision.

D'autres modifications à la LPRPDE sont prévues dans la *Loi protégeant les renseignements personnels des Canadiens*, qui se trouvait devant le Parlement à la fin de 2010. Cette loi propose, notamment, d'imposer de nouvelles obligations aux organisations assujetties à la LPRPDE, pour que celles-ci informent la commissaire à la protection de la vie privée et les intéressés de toute atteinte grave à la sécurité des données.

La création d'un système de notification obligatoire en cas d'atteinte à la sécurité des données serait une mesure qui favoriserait de manière considérable l'accroissement de la protection de la vie privée au Canada. Nous accusons un retard par rapport à plusieurs autres juridictions, qui ont déjà mis en place un tel système.

Cette mesure législative prévoit que les consommateurs devraient avoir le droit d'être mis au courant dans le cas où les renseignements qu'ils ont confiés à une organisation sont communiqués sans autorisation et s'il existe un risque substantiel qu'un tort important soit causé à leur portefeuille ou à leur réputation, à leurs occasions d'affaire ou d'emploi, ou à leur solvabilité.

Le Commissariat serait également mieux placé pour garantir que toutes les mesures sont prises pour corriger ou atténuer les préjudices. Ainsi, à la longue, nous serions en mesure de repérer les tendances et caractéristiques qui exigent une attention plus particulière, de sorte que les renseignements personnels des Canadiennes et Canadiens continuent d'être protégés.

En 2010, le Commissariat a commencé à se préparer pour le prochain examen de la LPRPDE, qui devrait commencer en 2011.

Nous avons commandé un rapport sur l'efficacité de notre modèle actuel d'ombudsman.

Nous avons également organisé des consultations publiques sur les enjeux pour la vie privée associés au suivi, au profilage et au ciblage en ligne des consommateurs par les spécialistes du marketing et d'autres entreprises, et sur les pratiques en matière d'infonuagique.

Le rapport et les consultations permettront d'étoffer notre contribution au prochain examen parlementaire de la LPRPDE.

Pour obtenir davantage de renseignements sur nos consultations publiques, voir le chapitre 2.

1.3 Appui aux organisations

SENSIBILISATION

À l'automne 2010, nous avons officiellement ouvert un bureau à Toronto. Les enquêtes portant sur des intimés de l'agglomération torontoise seront effectuées à partir de ce nouveau bureau, et nous profiterons de notre présence sur place pour multiplier nos liens avec des entreprises, des associations industrielles et d'autres intervenants de la région. Notre but est d'accroître la conformité aux dispositions de la LPRPDE dans le secteur privé grâce aux partenariats et à l'éducation.

Nous avons également amélioré notre outil en ligne pour aider les entreprises à protéger la vie privée de leurs clients. Cet instrument aide les entreprises à déterminer le volume d'information qu'elles sont censées avoir sur leurs clients et comment la protéger.

Pour obtenir davantage de renseignements sur les mesures que nous avons prises pour sensibiliser les organisations aux enjeux de la vie privée, voir le chapitre 5.

VÉRIFICATION

L'un des moyens à l'aide desquels nous aidons les entreprises privées à respecter la réglementation en matière de la protection de la vie privée est la vérification, par l'entremise de notre service de vérification, de leurs politiques, procédures et mécanismes

de contrôle visant à protéger la vie privée et les renseignements personnels de leurs clients.

En 2010, nous avons procédé à la vérification de Bureau en gros Ltée. À la suite de plaintes concernant des atteintes à la protection des renseignements personnels associées au retour de dispositifs de stockage d'information électronique et compte tenu des risques potentiels pour les consommateurs, nous avons décidé d'examiner les pratiques et les procédures du détaillant en matière de traitement des renseignements personnels.

La vérification, dont les résultats sont exposés au chapitre 3 du présent rapport, a révélé que les pratiques de Bureau en gros en matière de protection de la vie privée sont généralement bonnes, mais que la question de la gestion du retour des dispositifs de stockage de données n'était pas encore complètement réglée. Dans 15 des 17 magasins ayant fait l'objet d'une vérification, nous avons trouvé ce qui suit : des dispositifs qui avaient été réemballés après avoir été attesté exempts de données de clients alors qu'ils en contenaient encore; des dispositifs qui n'avaient pas été vérifiés par un responsable avant d'être remis dans les stocks; des dispositifs qui avaient été placés dans un contenant de marchandise retournée destinée à la vente sans avoir été débarrassés au préalable des données de clients

Nous avons recommandé une série de mesures pour aider Bureau en gros à respecter ses obligations en vertu de la LPRPDE.

1.4 Développement du savoir

CONSULTATIONS

Au printemps 2010, nous avons organisé des consultations publiques sur le suivi, le profilage, le ciblage en ligne et sur l'infonuagique. Nous avons reçu de nombreuses observations écrites et nous avons organisé trois événements publics à Toronto, à Montréal et à Calgary. L'objectif de ces consultations était d'en apprendre davantage sur certaines pratiques de l'industrie en la matière, d'explorer l'incidence de celles-ci sur la protection de la vie privée et de déterminer quelles étaient les attentes des Canadiennes et des Canadiens en ce qui concerne les mécanismes de protection de la vie privée par rapport à ces pratiques. Les consultations visaient également à étoffer notre contribution sur le prochain examen parlementaire de la LPRPDE.

Nous avons rédigé un rapport provisoire qui comporte le résumé de ce que nous avons entendu, notre point de vue sur la question et la manière dont nous envisageons l'avenir.

Nous avons publié cette ébauche de rapport dans le but de solliciter des commentaires et nous rédigerons un rapport définitif qui sera publié en 2011.

RECHERCHE

La recherche est de plus en plus importante à mesure que les technologies se complexifient et donnent lieu à de nouveaux risques pour la vie privée. Au cours des dernières années, nous avons consacré plus de ressources nous permettant de mieux cerner et comprendre les nouveaux enjeux soulevés par les technologies.

Au début de 2010, nous avons engagé deux informaticiens qualifiés et nous avons commencé à équiper un laboratoire interne pour faciliter leur travail. Cet investissement remplit deux objectifs : bâtir notre capacité de recherche sur les nouvelles technologies à l'interne et faciliter les enquêtes grâce à un important volet technologique.

Nous prévoyons consacrer davantage de ressources humaines et matérielles à cette importante fonction.

PROGRAMME DES CONTRIBUTIONS

Notre programme des contributions continue à financer des recherches de pointe et des projets de sensibilisation du public en matière de promotion et de protection de la vie privée. Nous avons ainsi versé plus de 2 millions de dollars pour financer plus de 60 initiatives dans tout le pays depuis 2004.

En 2010, 16 projets ont été financés. Les bénéficiaires poursuivent des recherches dans un certain nombre de secteurs d'intérêt primordial pour le Commissariat, notamment les suivants :

- la publicité ciblée en ligne;
- le partage de données entre les gouvernements et les organisations commerciales dans le cadre de programmes de sécurité nationale applicables aux frontières et dans les aéroports;
- la vidéosurveillance d'espaces publics par des organisations commerciales;
- les conséquences sur le plan du respect de la vie privée des sites Web de patients, des bases de données en ligne de dossiers médicaux et d'autres outils de la « Santé 2.0 ».

En matière de sensibilisation du public, le Programme permet de financer des projets visant à renseigner les Canadiennes et les Canadiens sur les enjeux relatifs aux cotes de solvabilité et à la vie privée et à les informer des répercussions des nouvelles technologies sur le droit des consommateurs à la vie privée et à sa protection.

FORMATION DES EMPLOYÉS

Compte tenu de la transformation rapide du domaine de la vie privée, le Commissariat reconnaît l'importance de la formation en matière de leadership, de gestion et de domaines spécialisés comme l'informatique et la vérification, et les techniques d'enquête. Ces compétences et ce savoir spécialisé sont indispensables à la réalisation de notre mandat. Nous avons donc pris des mesures pour attirer, former et garder au sein de l'organisation des personnes possédant les aptitudes et les capacités susceptibles de répondre à nos besoins organisationnels actuels et à venir.

1.5 Initiatives mondiales

Partout dans le monde, les autorités chargées de faire respecter la vie privée font face au même problème : comment protéger le mieux possible les renseignements personnels alors qu'ils sont en constant mouvement entre de multiples juridictions.

Les autorités chargées de la protection des données se rendent de plus en plus compte qu'elles ne peuvent s'appuyer uniquement sur les lois nationales pour protéger des données qui ne connaissent pas les frontières. En 2010, certaines mesures importantes ont été prises pour instaurer des cadres de coopération internationale.

GLOBAL PRIVACY ENFORCEMENT NETWORK (RÉSEAU MONDIAL D'EXÉCUTION DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS)

Des représentants de plusieurs autorités chargées de l'exécution des lois sur la protection de la vie privée se sont rassemblés à l'occasion d'une réunion organisée par l'Organisation de coopération et de développement économiques (OCDE) dans le but de lancer le Global Privacy Enforcement Network (GPEN).

Le Commissariat est l'un des membres fondateurs du réseau. À la fin de 2010, le GPEN comptait déjà plus de 20 membres sur quatre continents.

Le GPEN est un réseau informel d'autorités chargées de l'exécution des lois sur la protection des renseignements personnels dont l'objectif est de promouvoir la

coopération en partageant des renseignements sur les problèmes que soulève l'exécution des lois et en facilitant l'application transfrontalière des lois dans des domaines précis.

Le GPEN découle d'une recommandation formulée en 2007 par le Conseil de l'OCDE invitant les autorités à créer un réseau. La recommandation a été élaborée en collaboration avec un groupe de volontaires présidé par la commissaire Stoddart.

COOPÉRATION ÉCONOMIQUE DE LA ZONE ASIE-PACIFIQUE (APEC)

L'Accord de coopération de l'APEC sur la protection transfrontière des données est entré en vigueur en juillet 2010. Le Commissariat a participé à l'élaboration de l'Accord, auquel adhèrent également la Federal Trade Commission des États-Unis et des commissaires à la protection de la vie privée de l'Australie, de Hong Kong et de la Nouvelle-Zélande.

Comme le GPEN, l'Accord de l'APEC vise à encourager le partage d'information, mais il ne concerne que les autorités chargées de l'exécution des lois de la région de l'Asie-Pacifique et renvoie à une coopération transfrontalière plus officielle par le biais d'enquêtes et d'actions parallèles ou communes.

PARTAGE D'INFORMATION AVEC DES HOMOLOGUES ÉTRANGERS

Pour que l'exécution des lois soit efficace, il faut pouvoir partager de l'information avec d'autres organismes de protection des données. Notre capacité à partager de l'information était très restreinte, mais cela a changé grâce à l'adoption des modifications à la LPRPDE prévues dans le projet de loi antipourriel, qui a reçu la sanction royale en décembre 2010.

Ces modifications confèreront clairement au commissaire le pouvoir de collaborer et de partager de l'information avec ses homologues étrangers et avec ses collègues provinciaux.

Les dispositions de la nouvelle loi en matière de partage d'information instaurent un équilibre prudent. Nous ne pourrons partager d'information qu'en vertu d'une entente écrite limitant les données susceptibles d'être communiquées et leur usage. La commissaire pourra également conclure des ententes pour remplir d'autres tâches comme l'élaboration de normes, la réalisation de recherches communes et les échanges de personnel.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE)

L'Organisation de coopération et de développement économiques (OCDE) joue un rôle de premier plan dans l'élaboration de solutions aux problèmes liés à la protection des renseignements personnels et à la sécurité à l'échelle mondiale. Les activités du Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée visent à assurer une protection adéquate de l'information qui circule partout dans le monde et à favoriser la collaboration des autorités chargées de l'application de la loi.

Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'OCDE ont eu 30 ans en 2010. La LPRPDE incorpore le code type de l'Association canadienne de normalisation, qui est largement inspiré des lignes directrices de l'OCDE.

Pour marquer cet anniversaire, l'OCDE a organisé trois activités spéciales. La première portait sur l'élaboration des Lignes directrices, leur impact dans divers pays et leur rôle dans l'environnement actuel. La deuxième activité a eu lieu à Jérusalem, avant la Conférence internationale des commissaires à la protection des données et de la vie privée, et portait sur l'évolution du rôle de la personne dans la protection des données. La troisième activité portait sur les aspects économiques de la protection des données personnelles et de la vie privée.

La commissaire Stoddart dirige un groupe de volontaires qui a contribué à la planification de ces activités. Le Commissariat a également détaché un membre du personnel à l'OCDE pour participer à la rédaction d'un document de travail décrivant le nouveau contexte de la vie privée et les défis relatifs à la protection des renseignements personnels au XXI^{e} siècle. Ce document, qui devrait être rendu public en 2011, servira de document source en vue d'une analyse approfondie de la capacité des Lignes directrices à affronter les enjeux actuels.

Le Commissariat, en étroite collaboration avec le représentant du gouvernement du Canada – Industrie Canada – continuera de faciliter le travail important de l'OCDE dans le cadre de l'évaluation des Lignes directrices.

RÉSEAU IBÉROAMÉRICAIN DE LA PROTECTION DES DONNÉES

Nous avons également resserré nos liens avec le Réseau ibéroaméricain de la protection des données. Le Réseau a été créé dans le but de faciliter l'échange d'information entre les pays ibéroaméricains.

Lors de la Huitième réunion ibéroaméricaine sur la protection des données, qui s'est déroulée en septembre au Mexique, la commissaire adjointe Chantal Bernier a prononcé

un discours dans lequel elle faisait le point sur l'expérience du Canada au cours des 10 premières années d'application de la LPRPDE.

Le Commissariat a suivi de près le processus menant à l'adoption par le Mexique de sa nouvelle loi sur la protection des données dans le secteur privé (*Ley Federal de Protección de Datos Personales en Posesión de Particulares*), largement inspirée de la LPRPDE.

ORGANISATION INTERNATIONALE DE NORMALISATION

L'Organisation internationale de normalisation, mieux connue sous son sigle ISO, joue un rôle de premier plan dans l'élaboration de normes applicables à la protection de la vie privée dans le cadre de l'utilisation et du déploiement des technologies actuelles et émergentes.

Le sous-comité de l'ISO sur la sécurité de l'information dans les technologies – plus particulièrement le groupe de travail sur la gestion de l'identité et les technologies de la protection de la vie privée – est la pierre angulaire du développement des normes en matière de protection de la vie privée, y compris un cadre de protection de la vie privée et une architecture de référence de la protection de la vie privée.

Un membre important du Commissariat agit à titre de chef de la délégation canadienne et d'expert national au sein de ce groupe de travail, de même qu'à titre d'agent de liaison intérimaire de la Conférence internationale des commissaires à la protection des données et de la vie privée. Il représente aussi le Canada au sein d'un comité directeur sur la protection de la vie privée, qui se penche sur un grand éventail d'enjeux relatifs à la terminologie liée à la protection de la vie privée de même que sur des initiatives en cours de réalisation à l'ISO. Le comité a également organisé la première conférence internationale sur les normes en matière de protection de la vie privée, qui s'est tenue en Allemagne en octobre 2010. La conférence avait pour but de faciliter le partage d'information et la coordination entre les comités techniques de l'ISO chargés de l'élaboration de normes applicables à la protection de la vie privée et d'autres intervenants importants comme l'OCDE, l'APEC et les commissaires à la protection des données de différents pays.

FRANCOPHONIE

Notre participation aux travaux de l'Association francophone des autorités de protection des données personnelles (AFAPDP) continue d'être l'un des axes importants de nos activités internationales. L'AFAPDP, dont le Commissariat a été l'un des membres fondateurs en 2007, représente les autorités chargées de la protection des données dans les pays francophones.

En 2010, la commissaire adjointe Bernier a participé à l'assemblée annuelle de l'Association à Paris, où elle a présenté deux exposés. Elle y a parlé de l'expérience du Commissariat en ce qui a trait aux menaces que les nouvelles technologies font peser sur la vie privée, notamment dans le cyberespace, et à l'installation de scanners à ondes millimétriques dans les aéroports du Canada. Elle a également donné un aperçu du rôle du Commissariat dans le cadre d'une discussion sur les pratiques exemplaires en matière de protection des données dans les pays francophones.

Dans les années à venir, l'AFAPDP a l'intention d'aider davantage les pays en développement de la Francophonie à mesure qu'ils se doteront de nouveaux cadres législatifs pour protéger le droit à la vie privée de leurs citoyens. Le Commissariat appuiera vigoureusement ces efforts.

« ET POUR MON PROCHAIN NUMÉRO, JE VAIS DEVINER VOTRE NOM, VOTRE ADRESSE, VOTRE DATE DE NAISSANCE, LE SOLDE DE VOTRE COMPTE DE BANQUE ET TOUS LES DÉTAILS DE VOTRE DERNIER VOYAGE DANS LE SUD! »

CHAPITRE 2

Principal enjeu : la protection de la vie privée en ligne

Plus de quatre Canadiennes et Canadiens sur cinq sont désormais connectés à Internet, et la plupart d'entre eux sont en ligne tous les jours. Ils y vérifient la météo, organisent leurs voyages, cherchent l'âme sœur, magasinent, paient leurs factures et leurs impôts, regardent des vidéos, jouent, cherchent de l'information sur des produits et services et communiquent avec des amis, des membres de leurs familles et de parfaits étrangers.

Internet représente bien des choses : pratique, réconfortant et familier pour certains, frustrant et déroutant pour d'autres.

Mais une chose est sûre : toutes ces activités en ligne laissent derrière elles une piste de données continue.

L'ancien commissaire à la protection de la vie privée, Bruce Phillips, avait soulevé des préoccupations au sujet de cette piste dans son rapport annuel au Parlement de 1995-1996 : « Alors, il paraît que vous n'avez rien à cacher? – Tant mieux! Car du moment où vous vous réveillez à celui où vous vous endormez, vos moindres gestes sont notés, analysés, documentés et même commercialisés, et tout cela sans votre autorisation et sans même que vous le sachiez ».

Depuis, cette piste devient de plus en plus éloquente. En plus de révéler où nous sommes allés et ce que nous y avons fait, elle définit maintenant qui nous sommes.

Progressivement, cette piste se cristallise en un dossier numérique extrêmement détaillé qui présente un extraordinaire intérêt pour beaucoup de personnes et d'organisations.

Les gouvernements, qui se soucient de sécurité publique, vont sur Internet pour traquer d'éventuels malfaiteurs.

Les arnaqueurs et magouilleurs en tout genre y voient des possibilités de faire de l'argent.

Entre-temps, des entreprises légitimes veulent savoir ce que les Canadiennes et les Canadiens font en ligne pour les attirer vers des annonces publicitaires et des offres ciblées et pour utiliser judicieusement leur budget publicitaire. Tout en étant intéressant pour les gens disposés à recevoir de l'information utile adaptée à leurs intérêts, cela peut, par contre, constituer une ingérence pour ceux qui veulent qu'on les laisse tranquilles.

Nous vivons dans une ère que certains appellent l'ère des données massives, où l'économie numérique globale est alimentée par une circulation volumineuse de données à l'échelle internationale.

Grâce aux progrès des technologies de l'information et des communications et à la baisse des coûts de transmission et de stockage, ces transactions quotidiennes donnent souvent lieu à des flux transfrontaliers de données multipoints.

Les achats que nous faisons à l'étranger à l'aide d'une carte de crédit délivrée par une banque canadienne peuvent être traités dans un pays tiers et les données être l'objet de forage dans une quatrième juridiction.

Grâce à l'avènement de l'infonuagique, une entreprise canadienne peut employer un service en ligne fourni par une entreprise américaine pour traiter et conserver des renseignements personnels dans de multiples endroits à travers le monde. Ces renseignements peuvent ensuite servir aux employés de ladite entreprise canadienne depuis n'importe quel endroit au monde où il est possible de se connecter en réseau.

Internet et la technologie en général sont en train d'évoluer à une vitesse phénoménale.

Cette évolution rapide, conjuguée au caractère mondial des enjeux et au fait que les organisations et les personnes se démènent encore pour élaborer les règles d'engagement convenables, est telle qu'il est très difficile de protéger la vie privée dans cet environnement relativement nouveau.

Nous avons décidé d'aborder les enjeux de la protection de la vie privée en ligne à l'aide d'instruments comme les enquêtes, la recherche, la participation des entreprises, la sensibilisation du public et la collaboration avec nos partenaires internationaux.

En 2010, nous avons procédé à plusieurs enquêtes sur les pratiques d'organisations en ligne en matière de protection de la vie privée.

Les réseaux sociaux, qui, d'après les résultats de certaines études, relient désormais plus de la moitié des utilisateurs d'Internet au Canada, intéressent particulièrement le Commissariat.

En 2010, nous avons donné suite à notre enquête phare sur le plus grand réseau social mondial, Facebook, dont nous donnons une description à la rubrique 2.1.

Comme les Canadiennes et les Canadiens sont de plus en plus susceptibles de trouver l'âme sœur en ligne, il n'est pas surprenant que nous nous soyons également intéressés au site de rencontre eHarmony.

Nous avons également fait enquête sur le géant américain d'Internet, Google.

Nous nous sommes penchés plus particulièrement sur la collecte de données sans fil par des voitures recueillant de l'information pour la fonction cartographique Street View et nous avons constaté que l'entreprise avait enfreint la réglementation canadienne en matière de protection de la vie privée. Par ailleurs, nous avons dénoncé publiquement Google pour avoir lancé son service de réseautage social Buzz sans tenir compte du droit à la vie privée des utilisateurs de Gmail.

Notre message à tous les géants de la technologie a été clair : songez à la protection de la vie privée avant de lancer une nouvelle application, ne la laissez pas aux mains du hasard et des avocats!

Au printemps dernier, grâce à une première série de consultations auprès des consommateurs, nous avons cherché à nous faire une idée des répercussions de certaines nouvelles technologies sur la vie privée, notamment l'infonuagique et les technologies de suivi, de profilage et ciblage en ligne auxquelles ont recours les spécialistes du marketing et d'autres entreprises.

Nos consultations ont plus particulièrement porté sur les enjeux pour la protection de la vie privée associés aux enfants et aux adolescents, qui sont les utilisateurs les plus avides d'Internet et notamment des sites de réseautage social.

Nous avons également approfondi l'analyse de ces enjeux dans le cadre de nos activités de sensibilisation dans les écoles. Et nous avons formé un comité consultatif d'adolescents en provenance de toutes les régions du pays pour connaître leurs points de vue sur la protection de la vie privée à l'ère numérique.

Nous nous sommes interrogés sur les conséquences d'Internet pour la vie privée à d'autres égards durant l'année 2010. Par exemple, parallèlement à un document de consultation du gouvernement du Canada sur la Stratégie sur l'économie numérique du

Canada, nous avons rappelé l'importance de bien connaître le monde numérique pour aider les gens à protéger leur vie privée et à rester anonymes dans leurs communications en ligne.

Par ailleurs, nous avons salué l'adoption d'une loi essentielle à la lutte contre les pourriels, les messages textes en vrac et d'autres formes de communications électroniques indésirables. Les pourriels s'accompagnent de menaces telles que les espiogiciels, les maliciels et autres systèmes de hameçonnage, qui tendent à miner la confiance des consommateurs à l'égard des transactions en ligne. La nouvelle loi, qui a reçu la sanction royale en décembre, attribue au Commissariat un rôle d'application de la loi en partenariat avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence.

Le nouveau texte législatif apporte également des modifications à la LPRPDE. Il confère notamment au commissaire à la protection de la vie privée un pouvoir discrétionnaire élargi quant aux plaintes susceptibles ou non de donner lieu à une enquête, ce qui nous permettra d'aborder des questions plus complexes ou systémiques. Par ailleurs, la commissaire a désormais un pouvoir plus explicite en matière de partage d'information avec d'autres autorités chargées de l'application de la loi, au Canada comme à l'étranger.

Pour résumer, 2010 a été une année très chargée du côté des enjeux liés à la protection de la vie privée en ligne. En voici quelques-uns des points saillants.

2.1 Le suivi de Facebook

À l'automne, le Commissariat a annoncé que nous avions terminé un examen des transformations mises en place par Facebook à la suite de notre enquête sur le site et que les problèmes soulevés dans la plainte initiale avaient été résolus de façon satisfaisante.

La commissaire Stoddart a déclaré à cet égard que « les changements apportés par Facebook pour répondre aux inquiétudes soulevées dans le cadre de notre enquête de l'année dernière sont raisonnables et satisfont aux exigences établies par les lois canadiennes sur la protection des renseignements personnels. »

L'enquête, déclenchée par une plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (un groupe de défense d'intérêts publics), a donné lieu à des changements importants.

L'une des inquiétudes importantes soulevées au cours de l'enquête était l'accès presque illimité des concepteurs tiers de jeux et autres applications aux renseignements personnels des utilisateurs de Facebook.

En réponse à nos recommandations, Facebook a élaboré un modèle d'autorisation qui représente une nette amélioration. Les applications doivent désormais informer les utilisateurs du genre de données dont elles ont besoin pour fonctionner et demander l'autorisation pour y avoir accès et pour les utiliser. Des mesures techniques garantissent également que les applications ne peuvent avoir accès qu'aux renseignements dont elles ont effectivement besoin.

D'autres changements permettent d'informer clairement les utilisateurs des pratiques de Facebook en matière de protection de la vie privée. Le site a mis en place des paramètres simplifiés à cet égard et propose un outil permettant aux utilisateurs d'appliquer un paramètre de sécurité à chaque photo ou commentaire qu'ils affichent.

Nous avons fermé le dossier relatif à notre première enquête exhaustive sur Facebook, mais nous avons reçu d'autres plaintes sur de nouveaux problèmes, par exemple au sujet du système d'invitation à Facebook et des boutons Facebook « J'aime » sur d'autres sites. Ces questions étaient en cours d'enquête au moment de la rédaction du présent rapport.

DOSSIER FACEBOOK
Mai 2008 – Plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada.
Juillet 2009 – La commissaire à la protection de la vie privée annonce que son enquête a révélé un certain nombre de problèmes en matière de protection de la vie privée sur le site Facebook et que certains de ces problèmes ne sont toujours pas réglés. Elle demande à Facebook de prendre des mesures dans un délai de 30 jours.
Août 2009 – Facebook accepte d'adopter une série de modifications pour donner suite aux préoccupations de la commissaire. Facebook et le Commissariat établissent un calendrier d'un an pour la mise en œuvre de ces changements.
Septembre 2010 – La commissaire à la protection de la vie privée annonce qu'elle a terminé l'examen des changements mis en place par Facebook à la suite de l'enquête du Commissariat et que les problèmes ont été réglés de façon satisfaisante.
Actuellement : d'autres plaintes contre Facebook faisaient l'objet d'enquêtes en cours au moment de la rédaction du présent rapport.

2.2 Enquête sur eHarmony

La recherche de l'âme sœur au 21e siècle passe de plus en plus par l'écran d'ordinateur.

La popularité des sites de rencontre en ligne s'est accrue au cours des dernières années : ils sont désormais un moyen aussi courant que les présentations par ami interposé ou les rencontres dans les bars. Selon les statistiques du magazine *Harper*, les couples américains formés depuis 2007 sont probablement issus, à raison d'*un sur quatre*, d'une rencontre en ligne.

Selon les estimations, les recettes du secteur des sites de rencontre en ligne seraient de l'ordre de 3 à 4 milliards de dollars par an à l'échelle mondiale.

« Cela semble avoir supplanté toutes les autres formes de rencontre […]; je dirais que ce phénomène devenu très courant depuis les cinq dernières années », expliquait dans une entrevue accordée au *Washington Post* en 2010 Susan Frohlick, anthropologue culturelle de l'Université du Manitoba qui s'est penchée sur les rencontres en ligne.

La protection de la vie privée dans le contexte des rencontres en ligne, sur des sites où tant de gens affichent tant de renseignements personnels, est également devenue un problème très courant.

C'est dans ce contexte que nous avons procédé à notre première enquête sur les pratiques et les politiques des sites de rencontre en matière de protection de la vie privée en 2010.

Le site eHarmony est un site de rencontre américain très populaire, qui est disponible au Canada à l'adresse eHarmony.ca.

Pour s'inscrire, les utilisateurs doivent fournir un volume important de renseignements très personnels : ils doivent en effet remplir un questionnaire relationnel complet, qui comprend plus de 300 questions sur à peu près tout : le caractère, l'intelligence, l'apparence physique, la vitalité sexuelle, les antécédents familiaux et le revenu.

PLAINTE

Une femme membre de eHarmony a porté plainte auprès du Commissariat à la suite de sa décision de mettre fin à son abonnement et de demander au site de supprimer son compte en ligne.

Quelques jours plus tard, elle est allée vérifier si ses consignes avaient été appliquées et elle s'est rendu compte qu'elle avait toujours accès à son compte et que celui-ci contenait tous les renseignements personnels qu'elle avait déjà fournis.

Elle a contacté par la suite eHarmony à plusieurs reprises pour réitérer sa demande. Selon la plaignante, eHarmony lui a répondu que le compte n'était désormais plus accessible aux autres membres.

Cependant, eHarmony lui a dit qu'il n'était pas possible d'effacer entièrement toute trace de son abonnement ni de supprimer ses renseignements personnels.

Insatisfaite de cette réponse, elle a déposé une plainte auprès du Commissariat.

ENQUÊTE

Lorsque la plaignante a demandé au site de « supprimer » son profil, elle s'attendait à ce que son compte et tous ses renseignements personnels soient définitivement effacés des serveurs de eHarmony.

En réponse à sa demande, cependant, eHarmony a commencé par « fermer » – ou désactiver – son profil, le rendant inaccessible à des candidats potentiels.

La plaignante a rapidement fait savoir à eHarmony que ce n'était pas ce qu'elle voulait. C'est à ce moment-là qu'elle a appris que eHarmony ne supprimait pas définitivement les renseignements personnels de ses membres.

Notre enquête a révélé que l'option de fermer un compte n'était pas immédiatement accessible sur le site de eHarmony. On n'y trouvait pas non plus d'explication claire quant à la signification que eHarmony donnait à ce terme.

Par ailleurs, on n'y trouvait pas non plus d'option claire et distincte permettant de supprimer définitivement le profil.

Les responsables d'eHarmony ont déclaré qu'ils « anonymisaient » l'information dans les comptes fermés. C'est ce qu'ils ont fait dans le cas de la plaignante, mais sans expliquer à quelles conditions.

CONSERVATION DES DONNÉES

En vertu de la LPRPDE, les organisations doivent se doter de lignes directrices et de procédures concernant la conservation des renseignements personnels et y préciser les périodes minimales et maximales de conservation. Selon la loi, le site eHarmony n'est autorisé à conserver des renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées de la collecte.

Les responsables d'eHarmony ont déclaré qu'ils désactivaient les comptes et conservaient indéfiniment les données – au lieu de supprimer les comptes et l'information qui s'y trouvait – parce que 40 % des membres se réinscrivaient dans un délai de deux ans. Conserver les données épargne aux personnes qui veulent se réinscrire la tâche de remplir un nouveau questionnaire.

RECOMMANDATIONS

Nous estimons que eHarmony devrait donner clairement aux utilisateurs qui décident de mettre fin à leur abonnement le choix de désactiver le compte (temporairement) ou de le supprimer (définitivement).

Le site devrait également faire clairement la distinction entre ces deux options dans sa politique sur la protection de la vie privée.

Au cours de notre enquête, nous avons constaté que, si 40 % des membres ont tendance à réactiver des comptes dormants, la majorité — 60 % — *ne le font pas* et n'ont donc pas intérêt à ce qu'on conserve indéfiniment leurs renseignements personnels.

Nous avons par conséquent recommandé à eHarmony :

- d'élaborer et de mettre en œuvre une politique de conservation prévoyant que les renseignements personnels se trouvant dans des comptes désactivés soient supprimés, effacés ou anonymisés après une période raisonnable et d'en informer les utilisateurs;

- d'inclure une option de suppression des comptes;

- d'expliquer aux utilisateurs la différence entre la suppression et la désactivation des comptes et de rendre les deux options claires et faciles d'accès. Cette distinction devrait également apparaître dans la politique générale sur la protection de la vie privée.

RÉPONSE

Dans sa réponse, eHarmony a confirmé avoir pris ou être en train de prendre des mesures tenant compte de nos préoccupations, notamment :

- en fixant une période de conservation de deux ans pour les renseignements personnels recueillis par le site auprès des utilisateurs de son service;

- en proposant une procédure claire et efficace aux utilisateurs qui demandent à ce que leurs renseignements personnels soient supprimés;

- en fournissant aux utilisateurs de l'information claire sur la différence entre la désactivation et la suppression des comptes et sur la période de conservation des données par le site.

Les responsables d'eHarmony ont également expliqué au Commissariat comment et quand ils anonymisaient les données des utilisateurs, procédure qui permet effectivement de supprimer définitivement et irréversiblement dans les comptes tout moyen d'identifier l'utilisateur du compte. Ils nous ont confirmé que le compte de la plaignante avait été ainsi anonymisé et que les renseignements étaient désormais définitivement dépersonnalisés.

Ils ont également informé le Commissariat qu'ils avaient révisé et amélioré leurs procédures de réponse aux demandes concernant la protection de la vie privée.

CONCLUSION

Comme le site eHarmony offre désormais clairement aux utilisateurs la possibilité de supprimer complètement leur compte avant la fin des deux premières années, nous avons conclu que la période de conservation de deux ans par défaut pour les comptes inactifs était acceptable.

Au total, nous sommes satisfaits des réponses de eHarmony. Outre l'adoption d'une politique de conservation, les responsables ont clarifié les mécanismes de contrôle et amélioré les processus liés à la protection de la vie privée. La plainte a donc été jugée fondée et résolue.

AUTRES OBSERVATIONS

Nos inquiétudes à l'égard des politiques et pratiques en matière d'utilisation, de conservation et d'élimination des renseignements personnels dans les sites de rencontre en ligne ne se limitent aucunement à eHarmony.

Un rapide survol des autres sites révèle que certains n'ont même pas de politique sur la protection de la vie privée. Parmi ceux qui en ont, certains ne précisent pas ce qu'ils font des renseignements personnels lorsque les comptes ne sont plus actifs.

À moins qu'un site se débarrasse délibérément des renseignements personnels devenus inutiles pour l'utilisateur, l'information restera sur les serveurs. Cela ouvre la porte à une atteinte à la sécurité des renseignements personnels.

Nous invitons instamment les utilisateurs de sites de réseautage social – et notamment des sites de rencontre, en raison du volume de renseignements personnels qui y est recueilli – à prendre des mesures pour protéger leur vie privée. Ils devraient, par exemple, procéder comme suit :

- S'assurer que le site est doté d'une politique sur la protection de la vie privée et la lire avant de s'inscrire. La politique doit être claire et facile à comprendre. Elle doit préciser les types de renseignements personnels que le site recueille, comment il les utilise et comment il les protège.

- Vérifier si le site permet aux utilisateurs de supprimer leur profil et si la suppression est définitive. Certains sites permettent aux utilisateurs de fermer leur compte, mais cela ne fait que le désactiver de telle sorte qu'il ne soit plus accessible. Les renseignements personnels restent intacts dans la base de données, parfois indéfiniment.

- Vérifier si le site s'est doté d'une politique régissant la durée de conservation des renseignements personnels et vérifier le moment de la suppression et la manière dont celle-ci est effectuée, le cas échéant. Certains sites, par exemple, se contentent d'anonymiser les données après une période déterminée.

2.3 Google et les données Wi-Fi

En octobre 2010, le Commissariat a publié les résultats d'une enquête sur la collecte par Google inc. de données très confidentielles sur des réseaux sans fil non sécurisés.

Nous avons constaté que l'incident (des voitures de Google Street View ont inopportunément recueilli des renseignements personnels, comme des adresses de courriel, des noms d'utilisateur, des mots de passe, des numéros de téléphone et des adresses civiques) était le résultat de l'initiative d'un ingénieur et du fait que Google n'avait pas de mécanismes de contrôle des processus permettant de veiller à la protection de la vie privée.

Nous avons conclu que la collecte de ces données était illicite parce qu'elle allait à l'encontre des principes de base de la LPRPDE tels que le consentement éclairé de l'utilisateur à la collecte de ses renseignements personnels. L'incident constituait une grave violation du droit à la vie privée des Canadiennes et des Canadiens.

ENQUÊTE

Le Commissariat a amorcé cette enquêtes, car Google avait admis que ses voitures — qui photographient des quartiers pour l'application cartographique Google Street View — avaient, pendant plusieurs années, recueilli des données transmises par les réseaux sans fil. Ces réseaux, installés dans des foyers et des entreprises du Canada et du monde entier, n'étaient ni protégés par des mots de passe ni chiffrés.

Des spécialistes techniques du Commissariat se sont rendus dans les locaux de Google à Mountain View (Californie) pour examiner les données ainsi recueillies. Ils y ont procédé à une recherche automatisée de données semblant constituer des renseignements personnels.

Pour protéger la vie privée des intéressés, les spécialistes n'ont examiné manuellement qu'un petit échantillon de données signalées par le système de recherche automatisé.

Même à cette petite échelle, il était clair que certains des renseignements saisis étaient très confidentiels. Dans un document, par exemple, on a trouvé une liste de personnes souffrant de certaines maladies ainsi que leurs numéros de téléphone et leurs adresses.

Comme l'étude n'était pas censée être exhaustive, il est impossible de se faire une idée du volume de renseignements personnels recueillis sur les réseaux sans fil non chiffrés. Il est cependant probable que cela touche des milliers de Canadiennes et de Canadiens.

CODE INTÉGRÉ

Notre enquête a également révélé que Google recueillait ces renseignements personnels en raison d'un code intégré au logiciel employé pour capter les signaux Wi-Fi.

Le code a été élaboré en 2006 par un ingénieur de Google dans l'optique d'échantillonner toutes les catégories de données diffusées sur les réseaux Wi-Fi publics. Y sont incluses des lignes permettant la saisie de « données utiles » — cette expression renvoie au contenu des communications.

Comme Google n'avait pas pris de mesures pour mettre en place les protections nécessaires, le code a fini par être employé dans les voitures de Google Street View lorsque l'entreprise a décidé de recueillir de l'information sur la localisation de signaux radio Wi-Fi diffusés sur des réseaux publics. Ces renseignements ont été versés dans la base de données de ses services géodépendants.

Lorsque l'entreprise a décidé d'employer le code, l'ingénieur qui l'avait créé a fait état de répercussions superficielles sur la vie privée. Ces répercussions n'ont jamais été évaluées

par d'autres responsables de Google parce que l'ingénieur avait omis de transmettre les documents relatifs à la conception du code à l'avocat de l'entreprise chargé d'examiner les répercussions juridiques du projet Wi-Fi. Cela contrevenait à la politique de l'entreprise et découlait d'un manque flagrant de mécanismes de contrôle pour veiller au respect de la réglementation.

RECOMMANDATIONS

Compte tenu des résultats d'enquête, la commissaire a recommandé à Google d'adopter un modèle de gouvernance qui lui permette de se conformer aux lois en matière de protection des renseignements personnels. Ce modèle devrait comprendre des mesures de contrôle garantissant l'application de procédures nécessaires à la protection de la vie privée avant le lancement de nouveaux produits.

La commissaire a également recommandé à l'entreprise d'améliorer la formation de tous ses employés en matière de protection de la vie privée afin de favoriser la conformité. Elle a par ailleurs invité Google à désigner des responsables de la protection de la vie privée et de la conformité à la législation canadienne.

Elle a de plus recommandé l'élimination des données utiles canadiennes recueillies par l'entreprise, pourvu que cette opération ne soit pas interdite en raison d'une action judiciaire ou d'autres obligations en vertu de lois canadiennes ou américaines. Les données utiles canadiennes qui ne pouvaient pas être immédiatement supprimées devaient être sécurisées et leur accès, limité.

Google a pris des mesures à la suite de l'enquête du Commissariat. L'enquête était encore en cours au début de 2011, et le sera jusqu'au règlement complet de l'affaire par Google.

Le Commissariat s'est joint à plusieurs autorités internationales de la protection des données ayant mené une enquête sur l'incident de Google Wi-Fi. L'autorité espagnole a annoncé, à la fin de 2010, qu'elle avait entrepris une procédure d'infraction contre Google, une démarche qui pourrait éventuellement occasionner des amendes s'élevant à des centaines de milliers d'euros. Alors que nous nous préparons à publier le présent rapport, l'autorité française de protection des données a annoncé qu'elle avait imposé une amende d'environ 140 000 $CAN pour violation des lois françaises sur la protection de la vie privée.

Auparavant, le lancement du service Street View de Google avait aussi soulevé de grandes préoccupations à l'égard de la protection de la vie privée, et ce dans plusieurs pays, y compris au Canada.

2.4 Google Buzz

En avril, la commissaire Stoddart et neuf de ses homologues étrangers ont publié une lettre commune enjoignant Google inc. et d'autres entreprises internationales de respecter le droit des utilisateurs de leurs produits et services à la protection de leur vie privée.

La lettre, adressée à Eric Schmidt, alors président-directeur général de Google, et rendue publique au cours d'une conférence de presse très courue à Washington (D.C.), prévenait les organisations qu'elles devaient respecter les lois en matière de protection de la vie privée en vigueur dans chaque pays où elles proposaient de distribuer des produits et services en ligne.

Dans le cadre d'une collaboration sans précédent, les défenseurs de la vie privée — représentant 375 millions de personnes au Canada, en Europe, en Nouvelle-Zélande et en Israël — ont exprimé leur profonde inquiétude à l'égard des pratiques de Google.

Au cœur de leurs préoccupations se trouvait le lancement, deux mois auparavant, d'un réseau social du nom de Google Buzz. Pour créer Buzz, Google a simplement pris comme point de départ son service de messagerie Google Mail (ou Gmail). À partir de ce service privé de messagerie individuelle sur Internet, Google a automatiquement affecté à ses utilisateurs un réseau d'« amis » prélevés parmi les gens avec lesquels ils correspondaient le plus souvent par l'entremise de Gmail. Dans bien des cas, la liste a été rendue publique.

Ces utilisateurs n'ont cependant pas été suffisamment informés du fonctionnement de ce service et ils n'ont pas eu assez de temps pour donner un consentement éclairé. Cette façon de faire constitue une atteinte au principe mondialement reconnu selon lequel les gens doivent être en mesure de contrôler l'utilisation de leurs renseignements personnels.

Les utilisateurs de Gmail, évidemment inquiets que leurs renseignements personnels soient communiqués, ont vivement réagi. Google s'est excusée et a rapidement pris des mesures pour répondre aux critiques généralisées.

Les autorités de la protection des données ont cependant rappelé dans leur lettre que les problèmes associés à la mise en place de Google Buzz auraient dû être « évidents » pour l'entreprise. Elles ont invité Google et les organisations auxquelles sont confiés des renseignements personnels à intégrer les principes fondamentaux de la protection de la vie privée dès l'étape de la conception des nouveaux services en ligne au lieu d'attendre et de tester le produit sur le marché.

2.5 Loi antipourriel

Vers la fin de l'année, la loi antipourriel tant attendue a reçu la sanction royale. Cette loi réglemente non seulement l'envoi de messages électroniques commerciaux et d'autres formes de communications comme les messages textes commerciaux, mais interdit d'autres pratiques nocives comme la collecte d'adresses électroniques et les espiogiciels.

Le Commissariat appuie depuis longtemps l'adoption d'une telle loi parce que l'envoi de messages électroniques commerciaux non sollicités enfreint le principe de base de la protection de la vie privée, qui consiste à obtenir le consentement de l'intéressé avant de recueillir et d'utiliser ses renseignements personnels. Le pollupostage est également lié à l'hameçonnage, au vol d'identité et à d'autres atteintes à la vie privée.

En adoptant cette loi, le Canada a emboîté le pas aux autres pays du G8 ayant pris des mesures pour contrer cet assaut contre l'économie en ligne.

La nouvelle loi interdit les pourriels, dont les messages textes indésirables et autres formes de communications électroniques non sollicités, en renforçant notamment les exigences imposées aux expéditeurs en matière de consentement.

Le Commissariat partagera des pouvoirs de surveillance et d'application de la loi avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence.

Cette loi renforce le pouvoir du Commissariat de faire enquête sur la collecte non autorisée de renseignements personnels au moyen d'espiogiciels ou de la collecte d'adresses électroniques. Le CRTC s'occupera de l'envoi de messages électroniques commerciaux non sollicités, du réacheminement de communications sur Internet sans consentement et de l'installation sans consentement de programmes informatiques. De son côté, le Bureau de la concurrence s'occupera des pratiques de marketing trompeuses, dont les faux en-têtes et les contenus de site Web trompeurs. Les deux organismes sont habilités à imposer des sanctions importantes aux personnes et aux organisations qui enfreignent la loi.

Pour faciliter notre collaboration avec ces deux organismes, la loi confère au commissaire à la protection de la vie privée le pouvoir plus explicite de partager de l'information avec les autorités chargées de l'application de la loi. Ce pouvoir est vaste et permet de collaborer avec d'autres organismes de protection des données, au Canada et à l'étranger, pour lutter contre le pollupostage et d'autres pratiques.

La nouvelle loi, qui doit entrer en vigueur à l'automne 2011, confère également au commissaire un pouvoir discrétionnaire élargi lui permettant de rejeter ou d'abandonner une plainte.

Dès le début de 2011, nous avons commencé à élaborer une stratégie d'application de la loi, à élaborer des instruments de sensibilisation de la population et à engager du personnel pour que le Commissariat puisse assumer ses nouvelles responsabilités.

2.6 Consultations sur la protection de la vie privée des consommateurs

Au printemps 2010, le Commissariat a organisé des consultations sur des questions permettant, selon nous, de vérifier le degré de protection de la vie privée des consommateurs, de nos jours et dans un avenir rapproché. À mesure que les gens et les entreprises emploient les communications en ligne et tirent parti des avantages de l'ère numérique, les moyens par lesquels les sites en ligne utilisent les renseignements personnels à des fins lucratives doivent être examinés de près du point de vue du respect de la vie privée.

Nous avons retenu pour thèmes principaux le suivi, le profilage et le ciblage des consommateurs en ligne et l'infonuagique, parce que nous y voyons des tendances susceptibles d'avoir des répercussions sur la vie privée des Canadiennes et des Canadiens. Nous nous sommes intéressés notamment à la protection de la vie privée des enfants sur Internet.

Le but des consultations était d'en savoir plus sur certaines pratiques du secteur privé, d'analyser leurs répercussions sur la protection de la vie privée et de déterminer la protection à laquelle les Canadiennes et les Canadiens s'attendent à l'égard de ces pratiques.

Les consultations visaient également à susciter un débat sur l'incidence de l'évolution technologique sur la vie privée et à étoffer notre contribution au prochain examen de la LPRPDE, prévu pour 2011.

Nous avons reçu 32 observations écrites en réponse à notre avis de consultation. Nous avons également organisé trois événements publics retransmis sur le Web à Toronto, à Montréal et à Calgary.

SUIVI, PROFILAGE ET CIBLAGE EN LIGNE

En matière de suivi, de profilage et de ciblage en ligne, les participants aux consultations s'entendent généralement sur les problèmes, mais moins sur les solutions éventuelles.

L'effacement progressif de la frontière entre vie publique et vie privée et son effet sur la réputation des personnes ont occupé une grande place dans la discussion. Nous avons pris connaissance des préoccupations concernant les activités des enfants en ligne. Des enfants de tous âges sont présents sur Internet, et leurs renseignements personnels doivent être protégés. Les participants ont insisté sur le fait que la protection de la vie privée devait faire partie des stratégies de promotion de la culture et de la citoyenneté numériques.

La plupart des représentants d'entreprises estimaient que la LPRPDE protégeait adéquatement les renseignements personnels dans le contexte des nouvelles technologies et des nouveaux modèles opérationnels. D'autres participants étaient moins catégoriques.

Lorsque nous avons examiné les activités de suivi, de profilage et de ciblage en ligne par la lorgnette de la LPRPDE et des principes relatifs à l'équité dans le traitement de l'information, nous avons constaté la difficulté de déterminer ce qui est et ce qui n'est pas un renseignement personnel. Nous avons également constaté un manque de transparence à l'égard de ces activités et de ce que cela suppose du point de vue de l'obtention du consentement des intéressés, qui est une obligation en vertu de la LPRPDE.

Nous reconnaissons le travail accompli par les associations industrielles auprès de leurs membres pour les aider à respecter la LPRPDE. Des préoccupations ont été formulées au cours de nos consultations au sujet d'autres usages nouveaux – autres que la publicité comportementale – qui pourraient être faits des habitudes de furetage des consommateurs ou de leur réseautage social et de leurs données de localisation.

Nous invitons les associations industrielles à continuer de rappeler à leurs membres que le consentement des intéressés à l'égard de nouveaux usages de leurs données fait partie intégrante de la protection de la vie privée aux termes de la LPRPDE.

Il a beaucoup été question des problèmes des consommateurs dont les données en ligne sont conservées indéfiniment. Le Commissariat invite l'industrie à élaborer des moyens techniques pour régler ces problèmes.

Outre le problème de la conservation des données, l'accès à ses propres renseignements personnels et la vérification de leur exactitude sont deux dispositions importantes de la LPRPDE qui peuvent contribuer à régler certains problèmes de réputation découlant des

activités en ligne. Le Commissariat invite l'industrie à trouver des moyens novateurs de respecter les dispositions de la LPRPDE en matière d'accès, de correction et d'exactitude.

INFONUAGIQUE

L'infonuagique, un autre thème dans le cadre des consultations, renvoie à cette tendance croissante qui est de stocker les données par des fournisseurs tiers par l'entremise d'une connexion Internet.

La popularité de l'infonuagique s'explique par le fait qu'elle peut considérablement réduire le coût et la complexité de l'exploitation d'un centre de données local. Elle offre des capacités accrues en matière de protection et de sécurité des données si les fournisseurs emploient des moyens perfectionnés que les entreprises ne pourraient pas se permettre dans leurs propres centres de données.

L'infonuagique soulève des questions ayant trait aux juridictions et aux lois applicables.

La protection des renseignements personnels pose aussi un grave problème. Les données doivent être protégées durant leur transit sur Internet et lorsqu'elles sont stockées dans des endroits éloignés. De plus, comme les fournisseurs de services infonuagiques desservent de multiples clients en même temps, les données doivent être correctement séparées et protégées contre toute atteinte à la sécurité des renseignements personnels.

RAPPORT PROVISOIRE

Le 25 octobre 2010, nous avons publié une ébauche du rapport, qui contient ce que nous avons entendu au cours des consultations, ainsi que nos propres observations. Nous avons également sollicité les commentaires des intervenants contenu de cette ébauche, notamment ce qui suit :

- la gestion de l'identité en ligne;
- les mesures de base pour protéger les renseignements personnels des enfants;
- comment mieux expliquer les pratiques de protection de la vie privée;
- la nature des activités de suivi en ligne autres que la publicité comportementale;
- les mesures prises pour élaborer des normes de sécurité dans le contexte de l'infonuagique.

Nous avons reçu 12 observations écrites.

RAPPORT FINAL ET SUIVI

Au moment de préparer ce rapport annuel, nous nous attendions à publier notre rapport final sur les consultations au printemps 2011.

Nous avons beaucoup appris dans le cadre de cette initiative, mais il reste encore beaucoup à faire.

Par exemple, nous avons prévu des activités de recherche, que nous entreprendrons à court et à long terme, notamment un sondage et une recherche sur la différence entre l'information privée et l'information publique.

Nous avons l'intention de poursuivre nos activités de sensibilisation auprès des jeunes. Nous envisageons également des moyens de rejoindre les jeunes utilisateurs d'Internet, ainsi que les plus vieux qui sont de nouveaux venus dans l'environnement en ligne.

Nous continuerons de collaborer avec d'autres intervenants, par exemple des associations industrielles, des organisations et des promoteurs, nos homologues provinciaux et territoriaux et les ministères fédéraux, pour promouvoir une protection plus solide de la vie privée dans l'univers en ligne.

Sur notre site Web, nous continuons d'afficher de l'information à l'intention des personnes et des entreprises au sujet des questions que soulève le cyberespace, qu'il s'agisse de publicité comportementale, de témoins ou de l'infonuagique.

Les Canadiennes et les Canadiens ont besoin de sentir qu'ils peuvent accueillir la nouvelle technologie et appuyer les nouvelles entreprises sans renoncer au contrôle de leurs renseignements personnels. Les consultations de 2010 sur la protection de la vie privée des consommateurs constituent les prémisses de notre contribution à la discussion en cours sur les meilleurs moyens de la protéger dans les années à venir.

2.7 Consultations sur l'économie numérique

En juillet 2010, le Commissariat a déposé un mémoire officiel à l'intention du gouvernement du Canada dans le cadre des consultations sur l'économie numérique. Nous y avons fait valoir que le rythme rapide de l'innovation technologique avait des répercussions sur la vie privée et que la protection de la vie privée était indispensable au succès de l'économie numérique.

Nous avons rappelé que l'économie numérique du Canada est, en fait, une économie mondiale, compte tenu de la perméabilité des frontières à la circulation des données. Nous avons également examiné les nouveaux modèles opérationnels et les progrès technologiques, comme les services géodépendants, les dossiers de santé électroniques, l'analytique et les réseaux de capteurs qui composent ce qu'on appelle l'« Internet des choses », et nous en avons analysé les répercussions sur la vie privée.

Le document de consultation du gouvernement invitait les intéressés à donner leur avis sur le rôle que le gouvernement fédéral devrait jouer dans le soutien de l'économie numérique. On y proposait une série de mécanismes favorisant l'épanouissement de cette économie, par exemple la mise en place d'un cadre législatif ou stratégique, l'utilisation exemplaire des technologies numériques, le développement des compétences numériques, l'appui aux petites et moyennes entreprises; le financement de la recherche-développement.

Nous avons, dans notre mémoire, proposé des moyens d'améliorer la protection des renseignements personnels tout en favorisant l'innovation qui ferait du Canada un chef de file de l'économie numérique et de la protection de la vie privée.

Par exemple, nous avons souligné que les répercussions des nouvelles technologies sur la vie privée pourraient être traitées ou atténuées si des mesures de protection étaient intégrées dès l'étape de la conception. Nous avons également rappelé que la protection de la vie privée devait fait partie intégrante des modèles opérationnels reposant sur la technologie, et ce à partir d'une analyse approfondie des activités des entreprises. L'évaluation des facteurs relatifs à la vie privée est, selon nous, un instrument utile que le secteur privé devrait être invité à employer parce qu'il permet d'éviter les problèmes.

Pour intégrer la protection de la vie privée à l'étape de la conception et de la mise en œuvre des technologies, il faut, à notre avis, que les concepteurs et les utilisateurs (entreprises et personnes) possèdent les compétences numériques requises. L'une d'elles est la connaissance des principes de la protection de la vie privée.

Plus précisément, les Canadiennes et les Canadiens ont besoin de bien connaître les principes fondamentaux de la protection de la vie privée. Ils doivent adopter de bonnes habitudes en matière de protection des renseignements personnels et de gestion de leur réputation en ligne.

2.8 Sensibilisation des jeunes

Les jeunes sont parmi les utilisateurs les plus enthousiastes des technologies en ligne. Ils sont également prompts à essayer de nouvelles applications, parfois avant que les problèmes de protection de la vie privée soient identifiés et réglés. Compte tenu de leur disposition à envoyer des messages textes, à afficher de l'information sur Internet, à « tweeter », à avoir des « amis » et à partager des vidéos, on serait tenté de croire que la question de la vie privée ne les préoccupe guère.

Mais, comme l'attestent nos activités de sensibilisation, ce n'est pas nécessairement le cas.

En 2010, le personnel du Commissariat a fait 134 exposés devant un total de 21 000 personnes dans le secteur de l'éducation : des élèves d'écoles primaires et secondaires, mais aussi des collégiens, des professeurs, des policiers œuvrant dans les écoles et des parents.

Ce qui est ressorti systématiquement de nos échanges c'est que les jeunes veulent contrôler leur réputation en ligne. Ils veulent exercer un contrôle sur l'accès à leurs profils en ligne. Ils veulent savoir comment bloquer des communications indésirables sur les sites de réseautage social et comment savoir tout ce qui est affiché à leur sujet. Ils veulent aussi savoir ce qu'est la publicité ciblée et comment celle-ci influe sur la protection de leur vie privée.

Plusieurs sont avides de savoir comment supprimer définitivement leurs renseignements personnels, par exemple des réponses à des jeux-questionnaires en ligne qu'ils ne veulent plus voir circuler sur Internet et des choses qu'ils regrettent d'avoir affichées.

Et il y a l'éternelle question de savoir comment bloquer les demandes répétées de leur mère ou de leur père sur Facebook.

Dans le cadre de nos activités de sensibilisation dans le milieu de l'éducation, nous entendons souvent des histoires au sujet d'adolescents – et parfois d'adultes – qui peinent à trouver le comportement approprié à adopter sur les sites de réseautage social :

- Le directeur d'une école primaire nous a raconté qu'un de ses élèves avait créé un faux profil sur Facebook d'un autre élève de l'école et qu'il y avait ajouté de nombreux autres élèves comme « amis ». L'enfant ne comprenait pas que son geste pouvait faire du tort à la victime de sa farce.

- Le directeur d'une école nous a invités à faire un exposé après s'être aperçu que des jeunes filles de 7e et 8e années avaient fait circuler des images provocantes d'elles-mêmes dans les locaux de l'école. Interrogées, les fillettes ont déclaré avec

insistance que cela ne regardait pas le directeur, et la plupart des parents se sont dits d'accord avec elles.

- Un ressortissant d'un pays étranger s'est lié « d'amitié » avec de jeunes élèves atteintes d'autisme ou de déficience légère, prétendant qu'il vivait dans la même ville et avait environ leur âge. Certaines d'entre elles ont refusé de devenir son « amie » jusqu'à ce qu'il les menace en affirmant qu'il pouvait fermer leur compte Facebook. Une fois devenu leur « ami », il les a incitées à afficher des photos révélatrices d'elles-mêmes. Les policiers ont expliqué qu'ils avaient les mains liées parce que l'homme vivait à l'étranger.

- Des représentants de plusieurs écoles primaires et secondaires nous ont dit que des parents « pirataient » les comptes Facebook de leurs enfants et adressaient des messages offensants ou menaçants à d'autres enfants en conflit avec les leurs. Les directeurs disent aux parents que ce genre de comportement est inadmissible, mais les parents répondent que cela ne regarde pas l'école.

CONCLUSION

Les enjeux associés à l'univers en ligne joueront un rôle central dans nos activités au cours des prochaines années. Pour que le Commissariat demeure un défenseur efficace de la vie privée au Canada, c'est sur cet univers en ligne que nous devrons concentrer notre attention. Le respect de la loi et la sensibilisation du public à la protection de la vie privée dans le cyberespace resteront des priorités.

CHAPITRE 3

Principal enjeu : la destruction des données à l'ère numérique

Une vérification révèle que les données personnelles des clients de Bureau en gros demeurent à risque en cas d'atteintes à la protection des renseignements personnels

Le Commissariat à la protection de la vie privée du Canada a entamé une vérification de Bureau en gros Canada Ltée. (Bureau en gros) après avoir constaté plus d'une fois que le détaillant avait remis en vente des dispositifs de stockage retournés par des clients, où se trouvaient encore des renseignements personnels de nature délicate.

Dans le cadre de la vérification, nous avons testé les dispositifs de stockage d'information électroniques (ordinateurs portables, disques durs externes et clés USB) destinés à la revente et nous avons constaté que dans plusieurs cas, ils contenaient des renseignements personnels. Les dispositifs avaient été retournés à Bureau en gros, qui comptait les remettre en vente.

Une bonne part des renseignements personnels que nous avons trouvés étaient de nature assez délicate : des numéros d'assurance sociale, des numéros de passeport, des renseignements bancaires et des dossiers d'impôt.

À la suite d'une enquête réalisée par le Commissariat de 2004 à 2008, Bureau en gros avait pris des mesures pour améliorer ses procédures d'élimination des renseignements personnels des dispositifs en question, mais notre vérification a démontré que ces procédures n'étaient pas appliquées systématiquement et qu'elles n'étaient pas toujours efficaces en ce qui a trait à l'élimination des données des clients.

Notre vérification a donc révélé que Bureau en gros ne respectait pas ses obligations en vertu de la LPRPDE.

Le Commissariat a formulé une série de recommandations à Bureau en gros pour que l'entreprise se conforme davantage à la LPRPDE. Cette dernière a réagi à ces recommandations en spécifiant de quelle manière elle allait leur donner suite. Alors que les pratiques de Bureau en gros en matière de collecte, d'utilisation, de conservation et de destruction sont, de manière générale, conformes aux exigences de la LPRPDE, les problèmes relatifs à la gestion des dispositifs de stockage des données retournés n'avaient pas encore été réglés à la fin de la vérification.

CONTEXTE

Bureau en gros, dont le siège social se trouve à Richmond Hill (Ontario), est un important fournisseur d'appareils et de fournitures de bureau qui compte plus de 300 points de vente au détail au Canada.

De 2004 à 2008, le Commissariat a fait enquête à la suite de deux plaintes de clients de Bureau en gros alléguant que l'entreprise avait revendu un ordinateur et un agenda électronique qui avaient été retournés sans s'assurer que ceux-ci ne contenaient plus de renseignements personnels.

Après l'enquête réalisée sur ces deux plaintes, Bureau en gros a accepté de modifier sa façon de faire et d'instaurer une procédure complète de nettoyage et de restauration de tous les dispositifs de stockage de données retournés.

Malgré les engagements pris par l'entreprise, les médias ont fait état d'un incident semblable impliquant Bureau en gros en mars 2009.

Étant donné les deux plaintes et les articles parus dans les médias, le Commissariat a donc jugé qu'il était indiqué d'amorcer une vérification des pratiques de traitement des renseignements personnels chez Bureau en gros. Celle-ci a débuté en avril 2010.

Le commissaire à l'information et à la protection de la vie privée de l'Alberta a aussi fait enquête sur une plainte semblable et conclu que Bureau en gros avait enfreint la loi provinciale en ne protégeant pas certains renseignements personnels. L'entreprise avait, encore une fois, accepté de mettre en œuvre les recommandations du commissaire de l'Alberta.

Dans le cadre de cette vérification, nous avons examiné les politiques, les pratiques et les processus adoptés par l'entreprise en matière de gestion des renseignements personnels, notamment en ce qui a trait aux dispositifs de stockage de données retournés. Nous avons également examiné les processus et les formulaires ainsi que le programme de formation et de sensibilisation en matière de protection de la vie privée. Nous avons inspecté quelques points de vente au détail déterminés pour évaluer les mécanismes de

contrôle de la sécurité physique et informatique destinés à protéger les renseignements personnels. Nous avons aussi vérifié des dispositifs de stockage de données retournés par des clients et destinés à la revente pour déterminer si les renseignements personnels qu'ils contenaient avaient été supprimés.

Bureau en gros a fait l'objet d'une vérification en fonction de la LPRPDE, mais ses pratiques et ses normes n'ont pas été évaluées ni comparées à celles d'autres détaillants similaires.

UN ENJEU PRIMORDIAL

À chaque année se vend un nombre considérable d'ordinateurs de bureau, d'ordinateurs portables, de disques durs externes, de clés USB et d'appareils photo numériques au Canada. Ces appareils permettent de conserver d'énormes quantités de données, dont des renseignements personnels.

Beaucoup d'entreprises de vente au détail ont adopté une politique de « satisfaction garantie ou argent remis » pour leurs activités commerciales. En vertu de cette politique, les consommateurs peuvent acheter un article, l'utiliser un certain temps et le retourner pour obtenir un remboursement complet s'ils n'en sont pas satisfaits.

Par ailleurs, les appareils informatiques et électroniques sont généralement assujettis à une garantie du fabricant aux termes de laquelle le consommateur peut retourner un produit défectueux et en obtenir le remplacement. Certains de ces produits sont remis en état, réemballés et revendus.

Il y a donc un risque que ces produits soient revendus avant que les données du client n'aient été entièrement supprimées, ce qui peut menacer la protection des renseignements personnels des acheteurs précédents. La communication non autorisée de ces renseignements pourrait engendrer de graves conséquences, dont des pertes financières attribuables à l'usurpation d'identité ou à la fraude. Il s'agit donc d'une importante question d'intérêt public.

La LPRPDE stipule que les organisations doivent mettre en place des mesures de sécurité techniques, physiques et organisationnelles pour protéger les renseignements personnels des clients.

CONSTATATIONS

La vérification a révélé que les enjeux entourant la façon dont Bureau en gros gère les dispositifs de stockage d'information retournés par ses clients n'avaient pas encore été réglés.

En réaction à l'enquête menée par le Commissariat en 2008 à la suite d'une plainte, et pour atténuer le risque que d'autres atteintes à la sécurité des renseignements personnels ne se produisent, l'entreprise a révisé ses procédures de traitement des dispositifs informatiques et électroniques pouvant emmagasiner des données.

Toutefois, au cours de l'évaluation, nous avons découvert que les renseignements personnels couraient toujours un risque, et ce malgré ces changements.

Dans 15 des 17 succursales inspectées dans le cadre de la vérification, nous avons observé ce qui suit :

- des dispositifs avaient été remballés et déclarés nettoyés après avoir été vérifiés, alors que c'était faux;
- des dispositifs n'avaient pas été vérifiés par un responsable avant d'être replacés dans les stocks;
- des dispositifs avaient été mis dans la boîte « à retourner au fournisseur » sans que les données qu'ils contenaient aient été supprimées.

Nous avons testé 149 dispositifs de stockage d'information destinés à la revente qui avaient été soumis au préalable au processus de nettoyage et de restauration de Bureau en gros. Il s'agissait d'ordinateurs de bureau, d'ordinateurs portables, de disques durs externes et de cartes mémoire. Plus du tiers d'entre eux (54 sur 149) renfermaient encore des données de clients. Dans certains cas, les données résiduelles contenaient des renseignements personnels.

Certains dispositifs destinés à la revente contenaient des renseignements personnels de nature très délicate, par exemple :

- des noms, des adresses, des numéros d'assurance sociale, des numéros de carte d'assurance-maladie provinciale et des numéros de passeport;
- des antécédents professionnels, des diplômes et des relevés de notes;
- des renseignements sur les investissements personnels, des renseignements bancaires, des relevés de carte de crédit et des dossiers d'impôt;
- des permis de conduire, des cartes de résidence permanente et des visas d'étudiant.

Nous avons également examiné des appareils photo numériques, des systèmes de positionnement global (GPS), des lecteurs médias portables et des assistants numériques personnels. Les appareils photo et les lecteurs médias ne contenaient pas de renseignements personnels, mais deux des huit GPS n'avaient pas été remis dans leur état initial et contenaient des renseignements sur les déplacements et les adresses des anciens propriétaires.

La vérification a révélé que Bureau en gros ne prenait pas les mesures appropriées pour veiller à ce que les dispositifs de stockage retournés par ses clients soient entièrement nettoyés avant d'être revendus. La mise en place de nouvelles procédures n'avait pas permis de régler les problèmes que nous avions observés en 2008, lors de l'enquête menée à la suite d'une plainte déposée par un client.

La vérification a établi que les procédures de traitement des dispositifs de stockage retournés n'étaient pas toujours respectées. En outre, on a remarqué qu'un certain nombre de ces procédures, qui peuvent différer d'un fabricant à l'autre, ne garantissaient pas le nettoyage complet des données placées dans les dispositifs de stockage.

Dispositifs	Dispositifs vérifiés	Données associées à un client non décelées	Données associées à un client décelées
Ordinateurs (bureau et portables)	20	3	17
Disques durs externes	55	36	19
Disques durs internes	10	9	1
Clés USB	20	12	8
Cartes mémoire	44	35	9
Total	149	95	54

Les données ont-elles *vraiment* été éliminées?

La « suppression » des données d'un client dans un dispositif de stockage n'entraîne pas vraiment leur élimination réelle : l'endroit où elles se trouvaient devient tout simplement de l'espace libre. Les renseignements dont a besoin le disque dur pour trouver les données en question sont supprimés, mais *pas* les données en tant que telles.

Pour garantir l'élimination des données du client, il faut nettoyer. Ce processus permet d'écraser le contenu de l'espace qui était occupé auparavant par les données. À cette fin, des outils et des logiciels de sécurité existent déjà et des programmes pourraient être élaborés.

À moins que le dispositif n'ait été nettoyé, les données antérieurement « supprimées » peuvent être récupérées et restaurées dans un format lisible à l'aide d'instruments faciles à se procurer.

Au cours des tests auxquels nous avons procédé dans le cadre de la vérification, chaque dispositif a été branché à un ordinateur portable et examiné à l'aide de l'Explorateur Windows. Certains dispositifs contenaient des dossiers accessibles renfermant des renseignements personnels, tandis que d'autres semblaient avoir été nettoyés. Nous avons poursuivi l'examen de ces derniers pour y chercher du contenu dissimulé à l'aide de logiciels gratuits faciles à télécharger sur Internet.

AUTRES CONCLUSIONS DE LA VÉRIFICATION

Au cours de sa vérification, le Commissariat a examiné d'autres enjeux de protection de la vie privée et de sécurité liés aux mesures de protection et à la gestion des renseignements personnels.

MESURES DE SÉCURITÉ

- **Accès au système**

Nous avons constaté que l'utilisation de noms d'utilisateur communs et de mots de passe partagés sur quelques-uns des systèmes informatiques (les activités des utilisateurs du système informatique de Bureau en gros ne sont pas enregistrées) empêchait Bureau en gros de déterminer si le droit d'accès au système était exercé légitimement.

Sans être en mesure de surveiller qui accède au système, Bureau en gros ne peut garantir que les renseignements personnels des clients sont toujours utilisés et communiqués à des fins légitimes.

L'accès contrôlé au système informatique et aux données qu'il contient représente une mesure de sécurité importante pour la protection de la vie privée. Accorder l'accès uniquement à ceux dont le besoin de connaître est légitime permet d'atténuer le risque que des renseignements personnels soient compromis.

- **Rangement des documents**

Selon la politique de Bureau en gros, tous les renseignements personnels doivent être rangés dans un endroit sécurisé, c'est-à-dire dans des classeurs ou des pièces verrouillés, lorsqu'ils ne servent pas. Nous avons cependant découvert que 12 des 17 succursales visitées ne respectaient pas cette politique : nous y avons en effet trouvé des formulaires de livraison, de transfert et de commande spéciale remplis dans des classeurs non verrouillés. De plus, dans certaines de ces succursales, les formulaires de retour et de réparation n'étaient pas suffisamment protégés, et les dispositifs de stockage étaient conservés dans des meubles non verrouillés ou se trouvaient sur des étagères ouvertes ou des comptoirs de service.

- **Renseignements sur les clients dans des poubelles ou des bacs de recyclage**

Les renseignements sur les clients de Bureau en gros sont généralement détruits dans les succursales de l'entreprise qui ont recours aux services d'une entreprise spécialisée dans la destruction de documents. Les succursales sont munies de déchiqueteuses verrouillées. Il arrive cependant que des formulaires de commande contenant des renseignements personnels soient jetés dans des poubelles ou des bacs de recyclage plutôt que dans une déchiqueteuse.

SURVEILLANCE DE LA CONFORMITÉ DES POLITIQUES ET DES PROCÉDURES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Des politiques et des procédures exhaustives en matière de protection de la vie privée sont l'un des ingrédients essentiels d'un cadre de gestion solide de la protection de la vie privée. Elles doivent cependant faire l'objet d'une surveillance pour donner les résultats escomptés.

La conformité aux procédures et aux mécanismes de contrôle relatifs à la sécurité est évaluée en vertu du programme de vérification interne de Bureau en gros, mais nous avons découvert que l'entreprise ne surveille pas de manière systématique la collecte, la conservation et la suppression des renseignements personnels.

En ce qui concerne les dispositifs de stockage, la politique de retour de Bureau en gros stipule qu'un responsable doit vérifier si l'appareil a bien été nettoyé avant d'être revendu. Nous avons constaté que cela n'est pas fait systématiquement et que la plupart

des responsables tiennent pour acquis l'efficacité du processus de nettoyage et de restauration.

Quatorze des dix-sept succursales que nous avons visitées ont confirmé qu'il n'y avait pas d'inspections aléatoires et que les dispositifs destinés à la revente n'étaient pas testés dans le cadre du processus de vérification interne.

Une stratégie de contrôle continu, comprenant des vérifications internes, permettrait d'atténuer les risques pour la vie privée et de donner l'assurance que Bureau en gros remplit ses obligations en vertu de la LPRPDE dans le cadre de ses activités courantes.

GESTION DES RENSEIGNEMENTS PERSONNELS

- **Circulation transfrontalière de données**

Nous avons constaté que les commandes reçues par les centres d'appel de Bureau en gros, ainsi que les documents saisis par son service de copie et d'impression en ligne, sont acheminés et stockés aux États-Unis. Rien n'indique cependant que les clients en aient été informés.

De nos jours, l'économie mondiale interdépendante suppose une circulation internationale de l'information. Les transferts de données au-delà des frontières suscitent des craintes : où envoie-t-on les renseignements personnels, que leur arrive-t-il lorsqu'ils sont en transit et qu'en fait-on à destination? Comme nous l'expliquons dans nos Lignes directrices sur le traitement transfrontalier des données personnelles, les consommateurs auront davantage confiance si le transfert de leurs renseignements personnels est régi par des règles claires et transparentes.

- **Collecte inutile de données**

Nous avons constaté que certaines succursales de Bureau en gros faisaient des photocopies de documents d'identité délivrés par le gouvernement, par exemple des permis de conduire, des passeports et des cartes d'assurance-maladie, lorsque des clients font une demande de crédit. Ces documents contiennent des renseignements personnels, par exemple les caractéristiques physiques du titulaire, qui ne sont pas nécessaires lorsqu'il faut — pour des raisons légitimes d'établissement du crédit — vérifier l'identité du client et évaluer son dossier.

- **Documents conservés plus longtemps que nécessaire**

La LPRPDE prévoit qu'une organisation peut seulement conserver des renseignements personnels aussi longtemps qu'elle en a besoin pour atteindre ses objectifs. Notre

vérification a cependant révélé que des documents n'étaient pas assujettis à des échéances de conservation et d'élimination établis par Bureau en gros, que certains étaient conservés au-delà de l'échéance prévue et que d'autres étaient assortis d'échéances excessives et conservés indéfiniment.

Au cours de notre vérification, Bureau en gros a révisé ses échéances de conservation et d'élimination, des documents omis ont été ajoutés à la liste de ceux qui sont assujettis à des échéances de conservation et la période de conservation de certains documents a été raccourcie. Malgré ces mesures, le Commissariat est d'avis que la période de conservation des documents liés au service en ligne du centre de copie et d'impression de Bureau en gros est trop longue et ne respecte pas le principe de limitation de la conservation prévu par la LPRPDE.

- **Nettoyage des machines de bureau louées**

Les points de vente au détail de Bureau en gros louent des photocopieuses pour leurs services de copie et d'impression. Ces machines comportent des disques durs intégrés qui conservent des images de l'information traitée. À la fin du bail ou lorsqu'il faut remplacer les machines, les photocopieuses sont retournées au fournisseur.

Selon les ententes de location et les employés de Bureau en gros, la responsabilité de l'intégrité des données contenues dans le matériel incombe au fournisseur des machines. Cette responsabilité procure l'assurance que les disques durs sont nettoyés avant d'être éliminés, recyclés ou réutilisés.

Bureau en gros a confirmé qu'elle se fiait aux affirmations du fournisseur à cet égard et qu'elle n'avait pas procédé à un suivi indépendant dans le but de vérifier si les renseignements personnels de ses clients avaient été effacés.

RECOMMANDATIONS ET RÉPONSES

1. Bureau en gros devrait prévoir des examens de la conformité en matière de protection de la vie privée dans son programme de vérification interne.

Réponse de Bureau en gros

Bureau en gros accepte la recommandation. L'entreprise a modifié sa liste de vérification visant à prévenir les pertes afin de traiter plus en détail le stockage, la collecte, la conservation et l'élimination des renseignements personnels et d'autres aspects relatifs à la protection de la vie privée.

L'entreprise a établi un programme d'inspection hebdomadaire des salles de technologie pour veiller au respect de la vie privée. En outre, elle offre, dans toutes ses succursales, des formations sur la protection de la vie privée dans les salles de technologie afin de renforcer les pratiques exemplaires en matière de protection de la vie privée en ce qui a trait aux produits retournés par les clients ou à réparer. L'entreprise a créé une formation sur le code d'éthique et sur la gestion des renseignements personnels qui est obligatoire pour tous les associés, ce qui permet de mettre l'accent sur les priorités en matière de protection de la vie privée.

L'entreprise a centralisé ses services de récupération de données pour éviter que les succursales conservent des renseignements sur les clients dans la zone des services techniques. Elle a poursuivi le développement et la diffusion d'une application automatique qui repère les fichiers (pouvant appartenir aux clients) enregistrés par erreur sur les ordinateurs de la salle de technologie. Tous les fichiers repérés par cette application sont supprimés, conformément à la politique de l'entreprise interdisant de conserver dans ses succursales des données appartenant aux clients.

L'entreprise continuera d'établir de nouveaux examens de conformité pour soutenir ses politiques en matière de protection de la vie privée. Une équipe de gouvernance interfonctionnelle a été créée pour veiller au respect de la vie privée.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable en raison des changements effectués par Bureau en gros, qui prouvent que l'entreprise veillera à la conformité à la protection de la vie privée au moyen de vérifications internes. En allongeant sa liste de contrôle pour les vérifications internes, Bureau en gros sera mieux outillée pour repérer toute forme de non-conformité aux procédures dans ses magasins, de même que pour prévenir le traitement inapproprié des renseignements personnels. Enfin, Bureau en gros a créé une équipe de gouvernance sur la protection de la vie privée chargée de surveiller la conformité.

2. Bureau en gros devrait informer ses clients de toute utilisation ou communication éventuelles de leurs renseignements personnels, dont le transfert dans des pays étrangers.

Réponse de Bureau en gros

L'entreprise accepte la recommandation. L'entreprise modifiera en conséquence sa politique sur le droit à la vie privée d'ici le 15 mai 2011.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable.

3. Bureau en gros ne devrait pas conserver de photocopies de documents d'identité délivrés par le gouvernement dans le cadre de son programme de crédit interne.

Réponse de Bureau en gros

L'entreprise accepte la recommandation. La politique actuelle de l'entreprise interdit en toutes circonstances de reproduire et de conserver des documents d'identité délivrés par le gouvernement. L'entreprise a répété cette politique dans chacune de ses succursales et en poursuivra l'application.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable.

4. Bureau en gros devrait veiller à ce que les demandes de crédit interne soient traitées dans une zone privée.

Réponse de Bureau en gros

L'entreprise accepte la recommandation. L'entreprise a envoyé une directive à toutes ses succursales pour rappeler à ses associés l'obligation de respecter la vie privée à toutes les étapes du processus de demande de crédit et continuera d'appliquer cette politique.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable.

5. Bureau en gros devrait limiter la période de conservation des renseignements personnels associés aux commandes d'impression et de copie en ligne au temps nécessaire pour permettre au client de vérifier la qualité d'impression et de régler les problèmes s'il y a lieu.

Réponse de Bureau en gros

L'entreprise pense, comme le Commissariat, que les clients devraient être informés du fait que les demandes en ligne sont stockées pendant une période d'un an.

L'entreprise croit que la conservation des demandes en ligne des clients pour une durée d'un an est utile aux clients et aux entreprises, car l'information est stockée de façon sécuritaire par un tiers et régie par des ententes et des restrictions appropriées. La seule personne pouvant permettre la réutilisation ou la communication de l'information est le client lui-même. Toutefois, l'entreprise avisera dûment les clients de cette pratique, ce qui permettra à ces derniers de choisir les services de photocopie au comptoir s'ils le désirent.

Commentaires du Commissariat : À nos yeux, Bureau en gros n'a pas suivi notre recommandation selon laquelle les demandes en ligne d'impression ou de photocopie ne devraient être conservées que pendant une période permettant au client de réviser et de traiter tout problème relatif à la qualité de l'impression.

Même si Bureau en gros affirme qu'il informera ses clients que les demandes en ligne seront conservées pendant un an, nous sommes d'avis que cette information est stockée plus longtemps que le temps nécessaire, ce qui constitue une violation à l'obligation de la LPRPDE aux termes de laquelle les organisations ne doivent conserver les renseignements que pendant la période nécessaire ayant été préalablement déterminée. À partir du moment où le client a ramassé ses produits et qu'il en est satisfait, l'objectif de la collecte des renseignements personnels a été rempli et ceux-ci ne sont donc plus nécessaires.

Jusqu'à ce qu'elle modifie la longueur de la période de conservation conformément à notre recommandation, Bureau en gros manque à ses obligations aux termes de la LPRPDE.

6. Bureau en gros devrait veiller à ce que les ententes de location conclues avec des fournisseurs de matériel prévoient que ceux-ci remettent un certificat attestant la date à laquelle le disque dur a été nettoyé ou détruit.

Réponse de Bureau en gros

L'entreprise demandera des certificats de destruction à ses fournisseurs de matériel de photocopie. Cette demande a été communiquée aux fournisseurs actuels et sera ajoutée à toutes les prochaines ententes, nouvelles ou renouvelées, conclues avec les fournisseurs.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable.

7. Bureau en gros devrait examiner ses procédures et processus de nettoyage des dispositifs de stockage et mettre en place des mécanismes de contrôle améliorés pour éliminer les risques de communication de renseignements personnels.

Réponse de Bureau en gros

L'entreprise accepte la recommandation. À la suite d'une plainte déposée en 2008, l'entreprise a instauré une politique de nettoyage et de restauration de tout dispositif de stockage d'information (avec mémoire) ayant été retourné avant la revente. Dans le cas du nettoyage et de la restauration d'ordinateurs de bureau et d'ordinateurs portatifs, la compagnie suit les procédures et utilise les outils fournis par les fabricants. Ces procédures ne préservent que les logiciels d'origine expédiés par l'usine. Contrairement aux avertissements du fabricant selon lesquels ce processus efface tous les fichiers, les données peuvent être récupérées à l'aide d'un logiciel judiciaire. Aucun fabricant ne conseille d'écraser les données dans le cadre de son processus de nettoyage et de restauration recommandé. Dans certains cas, le processus d'écrasement peut endommager le disque dur de l'ordinateur et détruire le logiciel original provenant du fabricant (y compris les outils de nettoyage et de restauration du fabricant), ce qui aurait pour effet de rendre non viable sur le plan commercial l'utilisation universelle d'un tel processus.

L'équipe chargée de réaliser la vérification a été en mesure de récupérer, à l'aide d'un logiciel judiciaire, les données de quelques-uns des ordinateurs ayant été soumis au processus de nettoyage et de restauration recommandé par le fabricant. L'équipe de la vérification a recommandé la mise en place d'un processus de nettoyage et de restauration qui « écrase » toutes les données du client de manière à ce qu'aucune d'entre elles ne soit récupérable.

La compagnie étudie différents moyens d'éliminer les données stockées dans les produits retournés (pour faire en sorte qu'il soit impossible de récupérer les données à l'aide d'un logiciel judiciaire) sans endommager ou détruire les disques durs, les systèmes d'exploitation de valeur et d'autres outils fournis par le fabricant.

Commentaires du Commissariat : Au terme de la vérification, Bureau en gros n'avait pas complètement réglé le problème qui était à l'origine de la vérification – les plaintes déjà déposées selon lesquelles des renseignements personnels de clients se trouvant encore dans les dispositifs de stockage retournés n'avaient pas été supprimés de façon appropriée avant la revente de ces dispositifs.

Bien que la compagnie ait adopté une procédure de nettoyage et de restauration, celle-ci ne s'est pas avérée efficace pour l'ensemble des dispositifs.

Bureau en gros fait l'essai de divers moyens d'éliminer les données se trouvant dans les dispositifs, et ce sans endommager les systèmes d'exploitation. Toutefois, au moment de la rédaction du présent rapport, l'entreprise n'avait pas donné suite à notre demande d'information au sujet de la mise en place de mécanismes de contrôle en vue d'éliminer toute forme de risque relatif à la communication de renseignements personnels.

Sans la mise en place de notre recommandation concernant le nettoyage des données de clients, les renseignements personnels courent des risques et Bureau en gros manque à ses obligations aux termes de la LPRPDE.

La position du Commissariat est la suivante : si Bureau en gros n'est pas en mesure d'éliminer toutes les données de clients d'un dispositif donné, il est inacceptable de procéder à la revente de ce dispositif.

8. Bureau en gros devrait s'assurer que les renseignements personnels sont conservés dans des classeurs verrouillés ou des zones sécurisées, comme le prévoit la politique de l'entreprise.

Réponse de Bureau en gros

L'entreprise a réitéré ses politiques relatives au stockage des renseignements personnels et continuera de les appliquer. Elle a ajouté ce point à ses procédures de vérification interne.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable.

9. Bureau en gros devrait veiller à ce que les employés demeurent conscients de l'importance d'employer des méthodes sûres pour détruire les renseignements personnels des clients.

Réponse de Bureau en gros

L'entreprise a réitéré sa position auprès de ses employés et continuera d'appliquer ses politiques relatives à la destruction des données des clients. Elle a ajouté ce point à ses procédures de vérification interne.

Commentaires du Commissariat : Nous considérons que cette réponse est acceptable.

10. Bureau en gros devrait faire en sorte que les employés aient des codes d'accès uniques pour favoriser la responsabilisation des utilisateurs et atténuer le risque d'accès non autorisé aux données des clients.

Réponse de Bureau en gros

L'entreprise continue de chercher des solutions pratiques pour sécuriser l'accès et s'attend à ce qu'une application, présentement en développement, permette un accès personnalisé et sécurisé.

Soulignons que la politique actuelle de l'entreprise interdit de stocker des renseignements permettant d'identifier une personne sur un réseau partagé, à l'exception des systèmes utilisés à des fins opérationnelles. De plus, des politiques de contrôle d'accès relatives au serveur du point de vente situé dans les bureaux de direction des succursales sont en place et font l'objet d'une vérification. Les systèmes de l'entreprise comprennent la fermeture de session automatique et l'alternance de mots de passe génériques.

Commentaires du Commissariat : Nous considérons que l'engagement de Bureau en gros à trouver une solution constitue une réponse acceptable à notre recommandation concernant la mise en place d'une application d'accès unique. Nous avons demandé à Bureau en gros de fournir au Commissariat une conformation de la mise en œuvre de cette recommandation.

CONCLUSION

La LPRPDE impose des obligations aux entreprises privées en matière de gestion des renseignements personnels. Elle établit un équilibre entre le droit à la vie privée des personnes et la nécessité pour les entreprises de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins légitimes.

Dans le cadre de ses activités, Bureau en gros traite une grande quantité de renseignements personnels.

Les coordonnées des clients – nom, adresse, numéro de téléphone et données liées au paiement – sont au cœur des activités de collecte de l'entreprise. Mais cette dernière manipule également des renseignements personnels qui ne sont pas nécessaires pour répondre à ses besoins opérationnels courants.

À titre d'exemple, les demandes de copie et d'impression en ligne peuvent comprendre des renseignements délicats contenus dans des curriculum vitae ou des documents juridiques, par exemple des ententes de divorce et de garde d'enfants. Un ordinateur portable retourné ou confié pour réparation peut contenir des détails sur le niveau de scolarité, les troubles médicaux ou le passif financier du propriétaire de l'appareil.

Bureau en gros, qui a collaboré avec nous pendant la durée de la vérification, a adopté de nombreuses mesures positives pour améliorer la gestion des renseignements personnels : la mise en place de politiques et de procédures visant la gestion de l'information; une définition claire des rôles et des responsabilités de manière à ce que ceux-ci soient compris par l'ensemble du personnel; la mise sur pied de diverses approches, dont une formation obligatoire, en vue de sensibiliser le personnel.

Selon nous, Bureau en gros pourrait cependant tirer avantage d'une stratégie de surveillance permanente pour veiller à ce que ces pratiques et procédures en matière de vie privée soient respectées dans l'ensemble de l'entreprise.

Nous sommes satisfaits des réponses que l'entreprise a données à la suite de nos recommandations, sauf dans le cas de deux exceptions. En effet, tel qu'il a été mentionné précédemment, Bureau en gros ne satisfait toujours pas à ses obligations aux termes de la LPRPDE, soit celle concernant la période de conservation des demandes en ligne d'impression ou de photocopie et celle portant sur le processus de nettoyage des données.

Il est particulièrement décevant que le problème ayant donné lieu à la vérification n'ait pas été réglé.

À la suite des atteintes à la protection des renseignements personnels ayant mené au déclenchement des enquêtes sur la gestion des dispositifs de stockage retournés, Bureau en gros s'est engagée auprès du Commissariat à prendre des mesures correctives.

L'entreprise a donc fait des démarches pour améliorer ses procédures et ses mécanismes de contrôle, mais ceux-ci n'ont pas toujours été appliqués et ne se sont pas toujours avérés efficaces.

Les lacunes observées en 2008 existent encore. Tant que Bureau en gros ne règlera pas cette question, les renseignements personnels seront menacés.

Nous sommes d'avis que Bureau en gros et tout autre détaillant ne devraient pas remettre en vente un dispositif de stockage de données retourné s'ils sont incapables de supprimer toutes les données du client qui s'y trouvent. Nous sommes conscients que Bureau en gros fait présentement l'essai, à la suite de notre recommandation, de mécanismes de nettoyage de données plus efficaces.

Nous ferons un suivi auprès de Bureau en gros relativement à la mise en œuvre de nos recommandations. Nous avons d'ailleurs demandé à la compagnie de nous fournir, d'ici le 30 juin 2012, le rapport d'un tiers qui confirmerait que celle-ci leur a bel et bien donné suite.

Enfin, nous avons l'intention de continuer à surveiller les enjeux liés à la protection de la vie privée soulevés au cours de cette vérification et, au besoin, de faire un suivi auprès de l'industrie et auprès d'autres intervenants concernés.

CHAPITRE 4

Répondre aux préoccupations des Canadiennes et des Canadiens

Les demandes de renseignements et les enquêtes constituent l'essentiel de notre travail au Commissariat. Nous sommes en contact direct avec les Canadiennes et les Canadiens — que ce soit en répondant à leurs questions sur la protection de la vie privée ou en enquêtant sur les plaintes déposées à la suite de problèmes avec lesquels ils ont été aux prises lors de leurs communications avec diverses organisations.

Lors de ses présentations devant le Parlement pour discuter du renouvellement de sa nomination à la fin de 2010, la commissaire Stoddart a déclaré qu'au cours des trois prochaines années, elle entendait mettre l'accent notamment sur la prestation des services à la population canadienne. « En bout de ligne, le plus important pour moi, c'est que notre travail réponde aux besoins et aux attentes des Canadiennes et des Canadiens », a-t-elle souligné.

La commissaire a précisé qu'elle tenait à ce que les plaintes courantes — celles qui ne retiennent pas l'attention des médias — soient traitées avec autant de succès, car elles sont d'une importance vitale pour les personnes qui les déposent.

Le Commissariat a récemment entrepris la mise au point de son processus de traitement des demandes de renseignements et des plaintes en vue de mieux servir les Canadiennes et les Canadiens.

4.1 Demandes de renseignements

Les agents de demandes de renseignements offrent un service d'aide téléphonique aux Canadiennes et aux Canadiens ayant des questions au sujet de l'application des lois fédérales sur la protection de la vie privée dans leur vie de tous les jours.

En 2010, nous avons reçu 4 793 demandes de renseignements liées à la LPRPDE, soit environ la moitié de l'ensemble des demandes.

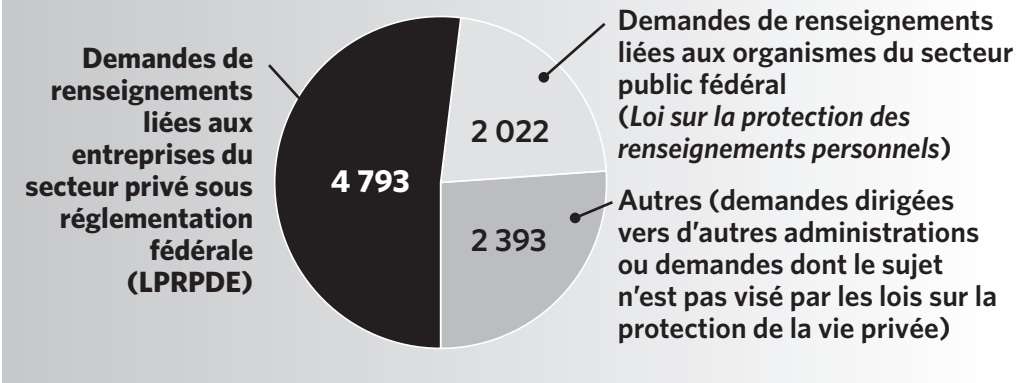
Le nombre de demandes de ce genre diminue graduellement depuis quelques années.

Par ailleurs, le nombre d'appels de fichiers sur notre site Web a énormément augmenté, ce qui semble indiquer que de plus en plus de gens visitent notre site afin d'y trouver les renseignements dont ils ont besoin au lieu de nous téléphoner pour les obtenir.

DEMANDES DE RENSEIGNEMENTS LIÉES À LA LPRPDE (SECTEUR PRIVÉ) REÇUES EN 2010

Par téléphone	4 081
Par écrit	712
Total	4 793

DEMANDES DE RENSEIGNEMENTS REÇUES EN 2010 (PAR TYPE)



Au cours du premier semestre de 2010, nous avons constaté une augmentation considérable du nombre d'appels de personnes ayant des questions à propos de Facebook et de Google Street View. Bon nombre d'entre elles avaient entendu parler de nos enquêtes sur les deux entreprises et voulaient savoir en quoi ces questions les touchaient personnellement. Par exemple, nous avons reçu des demandes de renseignements sur la façon de modifier son compte Facebook. Nous avons aussi reçu des demandes de personnes préoccupées par le fait qu'elles pouvaient voir leur maison sur Google Street View.

Le nombre d'appels à notre service téléphonique chargé de recevoir les demandes de renseignements a tendance à grimper dans les jours suivant le dévoilement par le Commissariat des résultats d'une enquête ou la diffusion par les médias de

commentaires de la commissaire. Fait intéressant à noter, toutefois, les appels portent souvent sur des sujets sans lien avec la nouvelle. La couverture médiatique entourant le Commissariat semble rappeler aux Canadiennes et aux Canadiens l'importance des questions relatives à la protection de leur vie privée au quotidien.

Nous continuons à recevoir des appels pratiquement tous les jours de personnes qui veulent savoir si des organisations comme les banques, les propriétaires ou les détaillants ont le droit de demander des numéros d'identification attribués par le gouvernement, tels le numéro de permis de conduire et le numéro d'assurance sociale.

Dans un cas en particulier, une personne nous a téléphoné pour déposer une plainte visant une compagnie d'assurance qui exigeait le numéro d'assurance sociale pour donner accès à son formulaire en ligne. L'agent de demandes de renseignements a communiqué avec la compagnie pour discuter de la question. Après l'entretien, l'entreprise a cessé de demander ce renseignement. De plus, le personnel de l'entreprise a reçu de la formation sur les utilisations acceptables du numéro d'assurance sociale.

Une autre question récurrente est la vérification de la solvabilité effectuée aux fins de l'établissement de la cote de crédit personnelle. Plusieurs personnes s'interrogeaient à savoir, par exemple, si les propriétaires avaient le droit d'exiger leur numéro d'assurance sociale pour procéder à la vérification de leur solvabilité comme condition préalable à la location d'un appartement.

SOLIDE SERVICE DE PREMIÈRE LIGNE

Nous avons considérablement modifié notre processus de recevabilité des plaintes au cours des deux dernières années.

De plus en plus, nous nous efforçons de régler les problèmes *avant* qu'ils ne fassent l'objet de plaintes officielles déposées au Commissariat.

Tout au long de 2010, le Commissariat a mis en œuvre des stratégies visant à renforcer le service offert à la population canadienne dès le début du processus de traitement des plaintes.

Les agents de demandes de renseignements sont souvent en mesure de répondre immédiatement aux questions ou aux préoccupations des appelants. Sinon, ils peuvent les diriger vers d'autres sources d'information ou d'aide, telles que le responsable de la protection de la vie privée d'une organisation.

De plus, ils demandent systématiquement aux appelants s'ils ont signalé le problème à l'organisation – et à la *bonne* personne au sein de l'organisation. Nous tenons à jour une

liste des responsables de la protection de la vie privée des grandes organisations au pays, et nous encourageons les gens à les appeler pour corriger toute situation problématique. Très souvent, un seul appel téléphonique suffit pour en arriver à un dénouement heureux.

Après une première analyse, lorsqu'il est manifeste que la question relève du champ de compétence du Commissariat, les agents de demandes de renseignements expliquent ce que celui-ci peut faire dans les limites du pouvoir qui lui est conféré en vertu de la LPRPDE.

Dans certains cas, ils font part aux appelants des résumés de conclusions d'enquêtes précédentes portant sur la question soulevée.

À mesure que nous acquérons de l'expérience dans la mise en œuvre de la LPRPDE, nous en tirons des leçons qui, souvent, peuvent s'appliquer à un ensemble de cas similaires – ce qui nous évite d'avoir à reprendre au complet le processus d'enquête officielle. Les résumés de conclusions d'enquêtes précédentes sont un outil important auquel nous recourons beaucoup pour informer le plaignant éventuel ou l'organisation des conclusions de cas antérieurs. Ils offrent également des pistes de solution.

Fortes de cette information, les personnes seront en mesure de s'adresser à nouveau à l'organisation pour revendiquer leurs droits.

Les agents de demandes de renseignements sont aussi chargés de recueillir le plus de renseignements possible auprès des plaignants éventuels afin que le Commissariat puisse déterminer la meilleure façon de répondre à leurs préoccupations.

Les demandes de renseignements non réglées sont acheminées au registraire des plaintes, qui décide s'il convient de traiter la préoccupation d'une personne en recourant au processus de règlement rapide ou à un enquêteur dans le cadre d'une plainte officielle.

4.2 Règlement rapide

À la fin de 2009, nous avons mis en place un mécanisme de règlement rapide dont s'occupent deux agents : l'un pour le secteur privé et l'autre pour le secteur public fédéral. Notre objectif visait à offrir un meilleur service aux Canadiennes et aux Canadiens en réglant les plaintes rapidement, grâce à une approche moins formelle que notre processus d'enquête officiel.

Lorsque des personnes communiquent avec nous au sujet d'un problème susceptible d'être réglé rapidement, elles sont dirigées vers un agent de règlement rapide.

Cet employé travaille à la fois avec le plaignant et l'organisation pour en arriver à une solution.

Le processus de règlement rapide est très efficace. Dans certains cas, un problème qui aurait pris des mois à régler dans le cadre du processus d'enquête officielle l'est en quelques jours. Nous avons entendu des commentaires très positifs sur le processus, aussi bien de la part des plaignants que des organisations.

PLAINTES FAISANT L'OBJET POUR RÈGLEMENT RAPIDE

En 2010, nous avons entamé l'examen de 112 plaintes pour règlement rapide. Nous avons réussi à trouver la solution appropriée dans la vaste majorité des cas.

Nous avons obtenu un règlement satisfaisant dans 62 cas; quatre autres demandes n'ont pas été résolues et ont été transférées au service des enquêtes; 46 étaient encore actives à la fin de l'exercice et seront traitées en 2011.[1]

Le fait que nous ayons pu trouver un règlement satisfaisant dans 62 des 66 dossiers traités en 2010 dans le cadre du processus de règlement rapide (soit plus de 90 % des cas) est très prometteur pour l'avenir.

En outre, nous avons réussi à régler rapidement 14 autres plaintes qui avaient été déposées en 2009.

Au total, 76 plaintes (62 examinées en 2010 et 14 en 2009) qui, auparavant, auraient probablement été résolues dans le cadre du long processus d'enquête l'ont été en relativement peu de temps.

Voilà une mesure positive pour la prestation d'un service rapide et efficace aux Canadiennes et aux Canadiens.

Bien entendu, les plaintes ne peuvent pas toutes être résolues ainsi. Celles qui soulèvent des questions complexes ou systémiques ou qui renvoient à des enjeux nouveaux continueront d'être traitées dans le cadre du processus d'enquête officielle.

1 *Nota* : Nos tableaux statistiques indiquent que nous avons examiné en 2010 108 plaintes plutôt que 112. Cet écart s'explique par le transfert, aux services des enquêtes, de quatre cas de règlement rapide, lesquels ont donc été mis dans la catégorie des plaintes reçues dans nos statistiques.

Le délai de traitement moyen des plaintes pour règlement rapide est de moins de trois mois, ce qui inclut le temps nécessaire pour obtenir du plaignant l'information requise pour entamer le processus. Nous modifierons notre définition des délais de traitement en 2011 pour fournir un portrait plus exact de nos résultats. Nous calculerons désormais le délai à partir de la date à laquelle nous aurons reçu tous les renseignements dont nous avons besoin pour commencer le travail.

Depuis que nous avons nommé deux agents aux dossiers pour règlement rapide, nous avons pu fermer ces dossiers plus vite que dans le passé. En 2009, par exemple, le délai de traitement moyen de ces dossiers était de six mois.

Le processus de règlement rapide est devenu un outil important pour donner suite promptement et efficacement aux préoccupations soulevées par les Canadiennes et les Canadiens auprès du Commissariat. Près du tiers de toutes les plaintes que nous avons traitées en 2010 l'ont été dans le cadre du processus de règlement rapide.

PLAINTES POUR RÈGLEMENT RAPIDE LIÉES À LA LPRPDE EN 2010

Résultats	Réglées rapidement	Envoyées pour enquête	En cours*	Total
Plaintes déposées en 2010	62	4**	46	**112**

* « En cours » signifie que le dossier de la plainte était encore ouvert à la fin de 2010.

** Dans certains de ces cas, les plaignants voulaient une enquête et une lettre officielle rendant compte de nos conclusions parce qu'en plus de déposer une plainte contre l'organisation, ils envisageaient d'intenter des poursuites.

DES CAS DE RÈGLEMENT RAPIDE EXEMPLAIRES

Une enquête de crédit suscite des inquiétudes

Une personne a remarqué dans son rapport de solvabilité qu'une société émettrice de cartes de crédit avait fait enquête sur elle, même si elle n'avait jamais eu affaire à l'entreprise. Elle était inquiète du fait que l'entreprise avait eu accès à ses renseignements personnels sans son consentement et que l'enquête pouvait avoir des répercussions négatives sur sa cote de solvabilité. Un agent de règlement rapide a pris contact avec la société émettrice de cartes de crédit et a appris que quelqu'un avait demandé frauduleusement une carte au nom du plaignant. La demande avait été rejetée parce que certains renseignements personnels fournis par le fraudeur étaient inexacts. Dans le cadre d'une demande de crédit, l'organisation vérifie en principe les antécédents du demandeur en matière de crédit. Cette vérification, qui est inscrite dans le rapport de solvabilité de l'intéressé et peut être consultée pendant des années par d'autres organismes de crédit, est susceptible d'affecter la cote de solvabilité de la personne concernée. La société émettrice de cartes de crédit ne pouvait pas supprimer la trace de la vérification de crédit, mais elle a pu l'inscrire en la désignant comme une « mise à jour », laquelle n'est accessible qu'au plaignant et n'a pas de répercussions sur sa cote de solvabilité. Le demandeur était content d'avoir eu accès à ces renseignements, qui lui ont permis, a-t-il dit, de comprendre la nécessité de suivre attentivement son rapport de solvabilité pour y vérifier l'existence éventuelle d'autres tentatives frauduleuses d'obtenir du crédit en son nom.

Le directeur d'une entreprise recourt aux coordonnées d'urgence sans raison valable

Un employé d'une petite entreprise de camionnage s'est adressé au Commissariat parce que l'entreprise avait utilisé des renseignements personnels se trouvant dans les dossiers du personnel. Le plaignant souhaitait garder l'anonymat, car il craignait des représailles si la question était traitée comme une plainte officielle. Il a déclaré que le directeur de l'entreprise avait envoyé une lettre à toutes les personnes que les chauffeurs avaient mentionnées comme personnes à contacter en cas d'urgence — conjoints, mères, frères, sœurs — pour leur donner des conseils sur la santé et la sécurité de ses employés. On pouvait notamment y lire ceci : « Nous comptons sur vous pour faire votre part afin que celui que vous aimez arrive reposé au travail. Vous pouvez commencer, par exemple, en gardant les listes de corvées ou d'autres tâches exigeantes sur les plans physique et émotionnel pour les jours où il ne travaille pas » [Traduction]. Un agent de règlement rapide a expliqué à l'entreprise de quelle façon la LPRPDE s'appliquait aux renseignements relatifs aux employés. La base de données qui avait été créée pour l'envoi de la lettre a été détruite, et l'entreprise s'est engagée à respecter les renseignements contenus dans les dossiers du personnel. L'employé s'est dit satisfait et était reconnaissant qu'on ait tenu son identité confidentielle.

Des avis répétés de changement d'adresse restent vains

Une personne s'est adressée au Commissariat après avoir demandé plusieurs fois à sa banque de changer son adresse et constaté que l'on continuait d'envoyer ses relevés bancaires à son ancienne adresse. Elle était très inquiète parce qu'elle croyait que les nouveaux occupants de son ancien domicile ouvraient son courrier. La banque pensait que l'affaire avait été réglée, mais, après examen avec l'agent de règlement rapide, elle a constaté que la correspondance était toujours envoyée à la mauvaise adresse et que les autres questions soulevées par la plaignante n'avaient pas été résolues. Grâce à notre intervention, la banque a réglé les problèmes de concert avec la plaignante et lui a même offert un dédommagement.

Un appel à un éditeur met fin à l'envoi de documents de marketing indésirables

Un couple a annulé son abonnement à une revue et demandé à ne plus avoir de contact avec l'éditeur. Les deux plaignants se sont lassés de continuer à recevoir des publicités. Un agent de règlement rapide s'est adressé à l'entreprise, qui a fait enquête et constaté que la demande n'avait pas été traitée. L'entreprise a tout de suite supprimé les données des plaignants dans sa base de données et ceux-ci se sont montrés satisfaits de la réponse immédiate.

Un numéro de téléphone non inscrit est largement diffusé en ligne

Une plaignante a été surprise et mécontente d'apprendre qu'une entreprise de location de voitures, à laquelle elle s'était adressée pour trouver une personne susceptible de reprendre son bail, avait affiché son numéro de téléphone confidentiel sur son site Web. D'autres entreprises automobiles avaient par la suite reproduit l'inscription. L'entreprise a fait savoir qu'elle avait supprimé les renseignements affichés. Mais l'information avait été saisie par un moteur de recherche populaire, et il s'est révélé difficile de supprimer l'information à ce niveau. Un agent de règlement rapide s'est adressé au fournisseur du moteur de recherche et a réussi à faire supprimer les renseignements personnels.

4.3 Plaintes

Au cours des dernières années, nous avons constaté une diminution du nombre de plaintes déposées au Commissariat. Cela s'explique surtout par le fait que nous avons réussi à aider des plaignants éventuels à régler leurs problèmes en s'adressant aux organisations concernées avant que l'affaire ne donne lieu à une plainte officielle. Il s'agit d'une tournure heureuse, car les longues enquêtes ne sont pas toujours la meilleure façon de répondre aux préoccupations des Canadiennes et des Canadiens en matière de protection de la vie privée. En traitant davantage de plaintes au moyen du règlement rapide et de la sensibilisation du public, nous pouvons ainsi consacrer nos ressources en matière d'enquêtes aux questions systémiques ayant de grandes répercussions à la grandeur du pays.

Comme nous l'avons expliqué à la rubrique 4.2, le processus de règlement rapide des plaintes nous a permis de trouver des solutions satisfaisantes dans des dizaines de cas qui, auparavant, auraient probablement été résolus par le recours au processus d'enquête.

En 2009, nous avons reçu 231 plaintes liées à la LPRPDE. En comparaison, en 2010, nous en avons reçu 207, ce qui inclut à la fois les cas résolus par le processus de règlement rapide (108) et ceux ayant été traités par le processus de plainte officielle (99). Cela représente une baisse annuelle de 10 %.

4.4 Plaintes par secteur d'activité

Ce sont encore une fois les institutions financières qui étaient visées par le plus grand nombre de plaintes, soit environ une plainte sur cinq (règlement rapide et plainte officielle).

Le nombre de plaintes déposées contre ce secteur d'activité ne signifie pas nécessairement que celui-ci ne respecte pas la LPRPDE, au contraire. Même si nos enquêtes ont circonscrit des aspects encore problématiques, notre expérience atteste que les institutions financières sont parmi les organisations dotées des meilleures politiques et pratiques en matière de protection de la vie privée.

La taille du secteur financier et l'énorme volume de transactions que supposent ses activités avec les Canadiennes et les Canadiens expliquent en grande partie le classement de ce secteur dans le cadre de la ventilation du nombre de plaintes par secteur d'activité.

PRINCIPAUX SECTEURS VISÉS PAR LES PLAINTES EN 2010

Secteur	Règlement rapide	Plaintes officielles	Total	Pourcentage de toutes les plaintes*
Secteur financier	21	24	45	22
Services	14	21	35	17
Assurance	13	14	27	13

* Le Commissariat a enregistré un total de 207 plaintes ayant fait l'objet d'un règlement rapide ou d'une plainte officielle.

Nota : L'annexe 2 présente des statistiques pour tous les secteurs d'activité ainsi que la définition des secteurs.

4.5 Types de plaintes reçues

L'utilisation et la communication de renseignements personnels de même que l'accès à ceux-ci ont été, une fois de plus, parmi les principales questions soulevées dans les plaintes adressées au Commissariat.

Nous avons cependant constaté une augmentation importante du nombre de plaintes liées aux au consentement, dont le pourcentage a doublé, passant de 10 % en 2009 à 20 % en 2010.

Il semble que cette augmentation globale soit attribuable en partie au nombre croissant de plaintes liées au cyberespace, où se pose souvent la question du consentement de l'intéressé concernant la collecte, l'utilisation et la communication de ses renseignements personnels. Onze des 20 plaintes reçues en 2010 alléguant des lacunes en ce qui a trait au consentement visaient le réseautage social, des sites Web ou des fournisseurs de services Internet.

TROIS PRINCIPAUX TYPES DE PLAINTES LIÉES À LA LPRPDE

Accès :	Utilisation et communication :	Consentement :
Plaintes concernant la difficulté d'accès à ses propres renseignements personnels	Plaintes concernant l'utilisation ou la communication inopportunes de renseignements personnels, sans consentement de l'intéressé, à des fins autres que celles pour lesquelles ils avaient été recueillis	Plainte concernant l'utilisation ou la communication de renseignements personnels sans le consentement éclairé de l'intéressé
22,2 %	22,2 %	20,2 %

4.6 Plaintes résolues

En tout, nous avons résolu 249 plaintes officielles en 2010, soit un nombre beaucoup moins élevé qu'en 2009, qui avait été une année atypique en raison d'un effort généralisé pour éliminer l'arriéré de dossiers.

Nous sommes heureux d'avoir réussi, dans la majorité des cas, à trouver une solution satisfaisante. Seulement 12 % des plaintes officielles ont été jugées fondées et non résolues, ce qui signifie que nous n'avons pas pu trouver de solution acceptable.

Dans ces cas non résolus, le Commissariat peut, s'il y a lieu, porter l'affaire devant la Cour fédérale. Si la commissaire estime que c'est dans l'intérêt public, elle a aussi le pouvoir discrétionnaire de dénoncer publiquement l'organisation incriminée dans le but d'informer les Canadiennes et les Canadiens des pratiques de l'entreprise en matière d'utilisation des renseignements. Le plaignant peut également choisir de porter lui-même l'affaire devant la Cour fédérale.

4.7 Aperçu des enquêtes de 2010

La section suivante porte sur des enquêtes parachevées en 2010. Des renseignements supplémentaires sur certaines d'entre elles se trouvent sur notre site Web.

La commissaire a rendu public le nom des organisations contre lesquelles des plaintes ont été déposées seulement lorsqu'il était dans l'intérêt public de le faire.

Soulignons que les enquêtes sur les organisations offrant des services Internet sont abordées au chapitre 2, la section spéciale sur la protection de la vie privée en ligne.

La présente partie fait ressortir certains risques pour les renseignements personnels que nous avons cernés au cours de nos enquêtes.

RISQUE : NE PAS OBTENIR LE CONSENTEMENT COMME IL SE DOIT

Une banque communique des renseignements personnels sans consentement

Un couple marié possédant des comptes de banque distincts et dont les membres ont décidé de ne pas échanger leurs renseignements financiers respectifs a décidé de faire un emprunt hypothécaire conjoint. Les époux ont donc invité une spécialiste de la banque pour les aider à remplir une demande.

Selon le plaignant et son épouse, pendant que la spécialiste des prêts hypothécaires se préparait, le plaignant a quitté la salle quelques minutes. Il croyait que la discussion ne commencerait pas avant son retour.

En son absence, la spécialiste a accédé à un rapport de solvabilité qu'elle croyait, à tort, être celui du plaignant, et elle l'a montré à l'épouse. Le rapport faisait état d'un endettement considérable.

Le plaignant affirme qu'à son retour dans la salle, son épouse était atterrée parce qu'elle pensait que son mari était très endetté sans qu'elle le sache.

On a plus tard découvert hors de tout doute que les renseignements étaient ceux du père de l'époux, qui porte le même nom. Lorsqu'il a été prouvé que le rapport de solvabilité n'était pas celui de l'époux, la spécialiste a tenté de rassurer l'épouse en lui montrant que le niveau d'endettement de son mari était négligeable. Le plaignant a affirmé que la spécialiste avait montré les renseignements sur sa marge de crédit et son solde de crédit à l'aide de son ordinateur portatif.

La spécialiste des prêts hypothécaires ne se souvenait pas d'avoir communiqué à l'épouse les renseignements concernant la marge de crédit et le compte de crédit du plaignant. Elle a soutenu qu'elle n'en aurait pas parlé tellement les soldes étaient négligeables.

La banque a reconnu que son employée a communiqué par erreur et de façon inappropriée le rapport de solvabilité du père du plaignant. Pour ce qui est des renseignements personnels du plaignant, la banque a soutenu que ce dernier avait implicitement consenti à ce que l'employée discute de ses renseignements de solvabilité avec son épouse.

Selon la banque, le spécialiste des prêts hypothécaires commence généralement par discuter avec les demandeurs conjoints pour les informer, entre autres, qu'il sera nécessaire de discuter de leurs actifs et de leurs dettes. Si l'une des parties présente une objection, le spécialiste offre des options. Par exemple, il peut s'entretenir individuellement avec chacun des conjoints pour parler de leurs dettes et de leurs actifs ou proposer une demande de prêt hypothécaire à un seul demandeur. Si aucune des parties ne s'oppose, la banque considère qu'il est raisonnable de poursuivre en se fondant sur le consentement implicite à la communication.

Dans ce cas précis, la banque croit que chacun des débiteurs hypothécaires avait implicitement accepté de discuter de sa situation financière en présence de l'autre.

Nous avons toutefois conclu que la banque n'avait pas fait un effort raisonnable pour s'assurer que les membres du couple comprennent pourquoi leurs renseignements financiers seraient communiqués l'un à l'autre dans le cas d'une demande d'emprunt hypothécaire conjoint. Dans cette affaire, la spécialiste n'a pas suivi la procédure habituelle de la banque, qui consiste à informer les demandeurs d'un prêt hypothécaire conjoint de la nécessité de discuter de leurs actifs et de leurs dettes.

De toute façon, même si la spécialiste a cru tout d'abord que les demandeurs avaient implicitement consenti à ce que leurs renseignements financiers soient communiqués, le fait que l'épouse ne connaissait manifestement pas la situation financière de son époux aurait dû lui faire comprendre que la présomption de consentement implicite n'était plus raisonnable ou appropriée. L'employée de la banque aurait au moins dû clarifier la situation avant de communiquer d'autres renseignements. Aux termes de l'enquête, le Commissariat était plutôt d'avis que la spécialiste avait communiqué les renseignements personnels du plaignant à son épouse.

Dans d'autres conclusions, le Commissariat a maintes fois soutenu le principe selon lequel les renseignements personnels ne doivent pas être communiqués aux conjoints sans leur consentement. Il a établi une norme de notification élevée à cet égard.

En résumé, la banque ne disposait pas de l'information lui permettant de conclure que le plaignant était consentant. Elle ne bénéficiait donc pas d'un consentement éclairé pour communiquer les renseignements personnels de ce dernier à son épouse.

Toutefois, l'incident en question découle d'une erreur ponctuelle d'une employée. La banque a réagi adéquatement et a adopté des pratiques raisonnables pour protéger les renseignements financiers des demandeurs d'un prêt hypothécaire conjoint. Par conséquent, la plainte a été jugée fondée et résolue.

RISQUE : UN EMPLOYÉ NE RESPECTE PAS LES PROCÉDURES

Un employé d'une banque communique des renseignements personnels

Une femme a présenté une plainte au Commissariat parce que sa banque avait, à deux reprises, communiqué ses renseignements personnels à l'avocat de l'ex-conjointe de son partenaire, et ce, à son insu et sans son consentement.

Le partenaire de la plaignante était en procédure de divorce. Dans le cadre de cette procédure, l'avocat de l'ex-conjointe a envoyé deux assignations à comparaître à la banque. La première demandait qu'un employé de la banque se présente devant les tribunaux et apporte une série de documents, dont les relevés de carte de crédit de la plaignante et le compte de crédit conjoint de son partenaire.

Un représentant de la banque s'est dûment présenté devant le tribunal et a remis les documents demandés en présence d'un juge.

La plaignante a ensuite fait part de ses préoccupations à la banque, soit du fait que ses renseignements personnels avaient été communiqués à l'avocat de l'ex-conjointe de son partenaire sans son consentement.

La banque a affirmé qu'elle avait envoyé par la poste un formulaire à la plaignante et à son partenaire pour obtenir leur consentement, mais qu'elle n'avait pas reçu de réponse. La plaignante a toutefois déclaré n'avoir reçu aucun formulaire avant son premier témoignage devant les tribunaux.

Avant sa deuxième comparution, la plaignante avait bel et bien reçu par la poste un formulaire de consentement envoyé par la banque. Elle avait cependant refusé que ses renseignements personnels soient communiqués dans le contexte de la procédure de divorce.

Selon la banque, à la suite de la seconde assignation à comparaître dans laquelle d'autres documents étaient demandés, un représentant de la banque s'était présenté devant les tribunaux avec les renseignements précisés. En attendant de témoigner devant le juge,

les avocats des parties au litige ont indiqué au représentant de la banque que celui-ci n'avait pas besoin de comparaître devant le juge et qu'il pouvait remettre les documents directement aux avocats (dont l'un était le partenaire de la plaignante, qui se représentait lui-même).

Le représentant de la banque a demandé le consentement écrit du partenaire de la plaignante pour communiquer les documents.

Le partenaire de la plaignante a accepté de communiquer l'information le concernant, mais il s'est toutefois opposé par écrit, sur le formulaire de consentement, à ce que les renseignements personnels de la plaignante soient communiqués. Le représentant de la banque a néanmoins communiqué les documents à l'avocat de l'ex-conjointe et au partenaire de la plaignante.

La banque a depuis affirmé qu'après s'être opposé par écrit, le partenaire de la plaignante s'est contredit en autorisant verbalement le représentant à communiquer l'information.

La banque soutient que le partenaire de la plaignante aurait dû, soit informer directement le juge qu'il s'opposait à cette démarche, soit avertir verbalement le représentant de la banque qu'il refusait la communication.

Dans ses observations au Commissariat, la banque a expliqué qu'elle était obligée de fournir les documents comprenant les renseignements personnels de la plaignante et qu'il n'était pas nécessaire d'obtenir le consentement de celle-ci. Selon ses procédures officielles relatives à la remise de documents à la cour dans le contexte d'une assignation à témoigner, la banque tente d'obtenir le consentement à la communication de l'information. Si elle échoue, un représentant comparaît devant les tribunaux et remet les documents demandés. Par contre, si les avocats conviennent qu'il n'est pas nécessaire de se présenter devant le juge, la banque demande le consentement écrit de l'avocat de son client et communique les documents.

Au cours de l'enquête, la banque a mis à jour ses procédures écrites concernant la production de documents dans le contexte d'une assignation à comparaître.

Dans le présent cas, les assignations à comparaître envoyées par l'avocat de l'ex-conjointe n'obligeaient pas la banque à lui fournir les documents; il suffisait qu'un représentant de la banque se présente en cour pour fournir des preuves et produire certains documents.

C'est pourquoi, en ce qui a trait à la seconde assignation, la banque *ne* pouvait *pas* invoquer une exception prévue dans la LPRPDE et aurait dû obtenir le consentement de la plaignante.

Selon nous, la banque dispose de bonnes procédures pour répondre à une assignation, mais le représentant ne les a pas suivies, car il a omis d'obtenir le consentement de la plaignante à la communication volontaire de l'information. Depuis cet incident, la banque veille à ce que ses employés connaissent les procédures appropriées.

La plainte était donc fondée et a été résolue.

RISQUE : COLLECTE EXCESSIVE DE RENSEIGNEMENTS PERSONNELS

Le vandalisme entraîne une surveillance excessive

Le plaignant était locataire d'un immeuble d'habitation de huit étages où se trouvaient 26 caméras de surveillance filmant l'intérieur du bâtiment et les environs en tout temps. Il soutient que la collecte de ses renseignements personnels au moyen de la vidéosurveillance est excessive et déraisonnable.

En visitant l'immeuble, nous avons constaté que les caméras, placées dans les corridors, captaient des images à l'intérieur de certains appartements quand les portes du corridor étaient ouvertes. De plus, une caméra située à l'avant de l'immeuble, à l'extérieur, filmait les piétons sur le trottoir.

Selon le gestionnaire immobilier, les caméras ont été installées en raison d'entrées par effraction et d'actes de vandalisme qui menaçaient la sécurité des locataires.

Aux termes de la LPRPDE, une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Le Commissariat a établi un critère en quatre parties permettant de déterminer si cette norme est respectée dans un contexte précis.

1. La mesure (dans ce cas-ci le système de vidéosurveillance) était-elle *nécessaire* pour répondre à un besoin réel?

Nous avons conclu que les entrées par effraction et les actes de vandalisme donnaient au gestionnaire immobilier un objectif légitime – protéger les locataires et les lieux – pour installer des caméras.

2. La mesure est-elle *efficace* pour répondre au besoin de sécurité?

Nous avons conclu que la présence de caméras avait un effet dissuasif contre le vandalisme et d'autres crimes. Le nombre d'incidents a considérablement diminué là où des caméras ont été installées.

3. La perte de vie privée est-elle *proportionnelle* aux avantages conférés?

Nous avons jugé qu'il fallait atteindre un meilleur équilibre entre le droit à la vie privée des locataires, d'une part, et la quantité et la nature de l'information recueillie actuellement par les caméras, d'autre part.

Par exemple, il était déraisonnablement envahissant de filmer constamment les portes des appartements des locataires, car les allées et venues quotidiennes de ces derniers peuvent facilement être surveillées. Il est tout aussi envahissant de filmer l'intérieur des appartements au moyen d'une surveillance permanente des corridors.

4. Existe-t-il un *moyen moins envahissant* d'atteindre le même but?

Le gestionnaire immobilier avait le devoir de protéger l'immeuble et il était ulcéré par les agissements de certains individus qui ont, par exemple, lancé des œufs sur le mur du vestibule et renversé des poubelles, mais cela ne justifie pas la prolifération des caméras. Celles-ci mettaient un frein aux agissements des malfaiteurs, mais avaient une incidence négative sur la vie privée des locataires respectueux de la loi. Il fallait envisager des moyens moins envahissants de parvenir au même but.

Nous avons formulé les recommandations suivantes à l'intention du gestionnaire immobilier : examiner l'emplacement de chaque caméra pour éviter qu'elles filment les endroits où les attentes sont plus élevées en matière de vie privée, par exemple à l'intérieur des appartements, à la porte d'entrée et sur le palier; s'assurer que les caméras ne filment pas les piétons; veiller à ce que celles-ci ne captent que des images permettant d'atteindre le but recherché, c'est-à-dire protéger la sécurité de l'immeuble et des locataires.

Nous avons aussi recommandé que les images ne soient examinées ou surveillées qu'à des fins de sécurité, et seulement après un incident.

Le gestionnaire immobilier a accepté de prendre les mesures suivantes :

- enlever et déplacer dans les puits d'escalier toutes les caméras situées dans les corridors;
- modifier l'orientation des caméras à l'extérieur de façon à ce qu'elles filment seulement à l'intérieur des limites de la propriété;
- veiller à ce que les vidéos soient examinées seulement si un problème de sécurité est signalé aux gestionnaires.

Nous avons donc conclu que la plainte était fondée et qu'elle avait été résolue en ce qui a trait à la collecte de renseignements personnels.

RISQUE : UTILISATION DE NUMÉROS D'ASSURANCE SOCIALE COMME DONNÉES D'IDENTIFICATION

Une plainte attire l'attention sur une préoccupation constante liée à un problème qui perdure depuis longtemps

Nous avons reçu une plainte selon laquelle une banque utilisait de façon inappropriée les numéros d'assurance sociale comme données d'identification lorsque les clients téléphonaient à son centre de services en matière d'investissements.

Le plaignant a communiqué avec le Commissariat après avoir appelé le centre de services et s'être fait demander son numéro d'assurance sociale complet dans le cadre du protocole d'identification de la banque.

Les numéros d'assurance sociale sont recueillis par des organisations comme les banques dans le seul but de signaler un revenu à l'administration fiscale.

Depuis longtemps, le Commissariat est d'avis que le numéro d'assurance sociale *ne* devrait *pas* être considéré comme une donnée d'identification et que les organisations devraient limiter

Numéros d'assurance sociale et protection de la vie privée

Le numéro d'assurance sociale a été créé en 1964 pour servir de numéro de compte client dans l'administration du Régime de pensions du Canada et les différents programmes d'assurance emploi. En 1967, l'actuelle Agence du revenu du Canada a commencé à utiliser le numéro pour les déclarations de revenus.

Le numéro d'assurance sociale est une donnée clé pour accéder à des renseignements personnels. Il peut, par exemple, servir à voler une identité. De pair avec d'autres renseignements personnels, le numéro d'assurance sociale pourrait être utilisé pour faire une demande de carte de crédit ou ouvrir un compte en banque, puis acheter frauduleusement des biens dispendieux et faire des chèques sans provision.

Seuls certains ministères et programmes gouvernementaux sont autorisés à recueillir et à utiliser le numéro d'assurance sociale. Cependant, aucune loi n'*interdit* aux organisations du secteur privé de le demander.

Certaines organisations continuent donc de demander le numéro d'assurance sociale parce qu'il s'agit d'une méthode d'identification simple. Elles sont nombreuses à l'utiliser comme numéro de compte client pour éviter d'avoir à établir leur propre système de numérotation.

C'est pourquoi le Commissariat a recommandé à plusieurs reprises que les organisations du secteur privé évitent de demander le numéro d'assurance sociale d'un consommateur et que les consommateurs ne fournissent pas ce numéro, *sauf* si l'organisation est légalement tenue de le faire.

la collecte, l'utilisation et la communication de ces numéros aux seules fins autorisées par la loi. Cette position est conforme à celle du gouvernement fédéral, selon laquelle le numéro d'assurance sociale ne devrait servir qu'à des fins autorisées par la loi.

La banque utilisait le numéro d'assurance sociale entier dans son processus d'identification par téléphone, mais elle a mis fin à cette pratique pendant le déroulement de l'enquête et ne demande plus que les trois derniers chiffres.

La plainte a donc été jugée fondée et résolue.

RISQUE : PROCÉDURES INADÉQUATES CONCERNANT LES DEMANDES D'ACCÈS

Une mauvaise gestion des demandes d'accès entraîne la suppression de renseignements personnels sans raison valable

Un homme a déposé une plainte au Commissariat parce que ses renseignements personnels avaient été supprimés par une importante entreprise de télécommunication en application de ses politiques courantes en matière de conservation et de retrait – même si le plaignant avait déjà demandé d'accéder à ces renseignements.

Une première demande du plaignant visant à avoir accès à ses renseignements personnels (des notes et des conversations enregistrées concernant plusieurs comptes, dont certains remontaient à 13 ans) a été ignorée malgré l'envoi de nombreux courriels de rappel pendant plusieurs mois.

Selon l'entreprise, un de ses bureaux a mal acheminé et traité la première demande. On a alors invité la personne à faire une nouvelle demande, ce qu'il fit, mais cette fois en l'adressant précisément au responsable de la protection de la vie privée de l'entreprise.

Or, la firme n'a pas donné suite à la seconde demande dans un délai de trente jours, comme l'exige la LPRPDE. Toutefois, cinq semaines après l'envoi de cette demande, elle a communiqué avec le client afin de lui demander l'autorisation de proroger le délai en raison du volume important de renseignements demandés.

Plus de soixante-dix jours après l'envoi de la deuxième demande, la firme a envoyé au plaignant des copies de l'ensemble des notes concernant ses comptes. Ce retard était attribuable en partie au décodage et à la transcription de données enregistrées dans un format qui n'était plus utilisé par le système informatique actuel de l'entreprise.

Cependant, les documents envoyés ne comprenaient pas les enregistrements d'appels du client relatifs à ses comptes. L'entreprise nous a informés qu'avant de recevoir la

deuxième demande d'accès, elle avait effacé tous les enregistrements datant de plus de six mois, conformément à sa politique de conservation.

Même si l'entreprise avait en sa possession des enregistrements d'appels du client qui dataient de six mois avant sa première demande (mal traitée), ceux-ci avaient depuis été détruits, conformément à la politique habituelle de conservation.

Par conséquent, la personne a définitivement perdu accès à certains de ses renseignements personnels. La suppression aurait pu être évitée si la firme avait traité correctement la première demande du plaignant, ou si elle avait au moins répondu aux messages subséquents en cas de doute.

Au cours de l'enquête, l'entreprise s'est engagée à améliorer ses politiques et ses pratiques relatives aux demandes d'accès des clients et à prévoir une exception, dans sa politique de conservation, pour les renseignements personnels faisant l'objet d'une demande d'accès non résolue.

Nous avons conclu que les plaintes concernant tant le délai de traitement que l'accès étaient fondées et résolues.

PLAINTES NON RÉSOLUES

Nous sommes généralement en mesure de régler les problèmes de façon satisfaisante au moyen de notre processus d'enquête. La grande majorité des organisations répondent favorablement à nos recommandations.

Toutefois, lorsqu'une société refuse de suivre nos recommandations, nous pouvons demander à la Cour fédérale de rendre une ordonnance pour l'obliger à se conformer et à offrir un dédommagement, s'il y a lieu. La commissaire peut également dévoiler le nom des entreprises qui ont fait l'objet d'une enquête si elle juge qu'il est dans l'intérêt public de le faire dans les circonstances.

Les résumés de conclusions d'enquête suivants donnent des exemples de plaintes qui n'ont pu être résolues de façon satisfaisante.

Une enquête met en évidence la non-conformité de l'Autorité aéroportuaire avec la LPRPDE

Un homme a déposé une plainte auprès du Commissariat parce qu'il était préoccupé par la collecte de renseignements personnels sans consentement effectuée par une employée de l'Autorité aéroportuaire du Grand Toronto (GTAA), et du manquement de la GTAA à donner accès au plaignant à ses renseignements personnels.

Selon une des allégations faites par le plaignant, son ex-conjointe, une employée de la GTAA, a utilisé de façon inappropriée de l'équipement du GTAA pour recueillir des photographies de lui et de sa famille pendant leur séjour à l'aéroport Pearson de Toronto. Le plaignant a contacté le GTAA pour faire part à l'organisation de ses préoccupations relatives à la vie privée. Le GTAA a mené sa propre enquête interne. Le plaignant a également demandé l'accès à ses renseignements personnels détenus par la GTAA. Insatisfait de la manière dont la GTAA avait mené l'enquête et traité sa demande d'accès, le plaignant a porté plainte auprès du Commissariat.

Nous avons conclu, à la suite de notre enquête, que les mesures prises par la GTAA n'étaient pas conformes à la LPRPDE. Nous avons découvert que les photographies avaient été prises sans le consentement et à l'insu de la personne concernée, et à des fins qui dépassaient largement les normes de surveillance, ce qui constituait, selon nous, un usage inapproprié. De plus, nous avons découvert que l'autorité aéroportuaire avait pris plus de deux mois – soit bien au-delà des trente jours prescrits – pour répondre à la demande d'accès du plaignant. Nous savions également que la GTAA avait en sa possession plus de renseignements personnels au sujet du plaignant que ceux fournis dans le cadre de sa réponse tardive à la demande d'accès.

Nous avons formulé les recommandations suivantes à la GTAA :

- fournir une liste exhaustive des renseignements personnels du plaignant, quel que soit leur format, qu'elle avait sous son contrôle jusqu'au jour de la demande d'accès du plaignant;

- mettre en place un système au moyen duquel tous les ordinateurs à utilisation mixte étant reliés à l'équipement de vidéosurveillance soient munis d'une procédure d'ouverture de session pour les employés qui les utilisent;

- élaborer une politique sur la vidéosurveillance à l'intention des employés et veiller à ce qu'elle soit lue et signée par les employés ayant accès à l'équipement de surveillance.

La GTAA a fourni une réponse aux recommandations du Commissariat. Cependant, nous avons jugé cette réponse insatisfaisante et avons conclu que la plainte était fondée. Compte tenu du caractère fondé et non résolu de la plainte, la commissaire à la protection de la vie privée a déposé une requête devant la Cour fédérale en vertu de l'article 15 de la LPRPDE. Les détails de cette requête figurent au chapitre 6.

Optique Laurier communique les renseignements personnels d'un client de façon inappropriée

Un client ayant demandé un remboursement par écrit après avoir acquis deux paires de lunettes prescrites qui ne répondaient pas à ses attentes a été très surpris d'apprendre qu'Optique Laurier avait envoyé une copie de sa réponse à dix parties.

L'homme s'est plaint au Commissariat que la chaîne d'optométristes, qui possède des succursales en Ontario et au Québec, avait communiqué ses renseignements personnels sans son consentement et avait par la suite omis de lui donner accès à ceux-ci.

L'homme a reçu deux prescriptions d'Optique Laurier et a jugé que ni l'une ni l'autre ne répondait à ses attentes. Il a donc obtenu une prescription d'un optométriste indépendant travaillant ailleurs.

Après avoir reçu la demande de remboursement, Optique Laurier a porté plainte contre l'optométriste indépendant devant l'Ordre des optométristes de l'Ontario. L'entreprise affirmait que l'optométriste avait donné au plaignant une information fausse en affirmant qu'Optique Laurier n'avait pas effectué un examen de la vue adéquat.

Dans sa réponse écrite à la demande de remboursement, Optique Laurier avait inscrit l'adresse domiciliaire, le numéro de téléphone et les détails des trois prescriptions du plaignant ainsi qu'une description du différend concernant celles-ci. Le plaignant considère que la réponse comprend de fausses déclarations nuisant à sa réputation. La lettre mentionne également qu'Optique Laurier demanderait à deux autres ordres professionnels et aux deux plus grands laboratoires de fabrication de lunettes du Canada d'évaluer les trois prescriptions et de formuler des opinions neutres.

Une copie de la lettre a été envoyée à dix parties, y compris divers dirigeants d'Optique Laurier, l'Ordre des optométristes de l'Ontario, l'Ordre des opticiens de l'Ontario, l'optométriste indépendant, l'entreprise qui avait fabriqué les lunettes du plaignant et un autre fabricant de lunettes.

Le plaignant a aussi demandé d'accéder à ses renseignements personnels détenus par Optique Laurier, mais il n'a reçu aucun document.

Après son enquête, le Commissariat a conclu que les plaintes relatives à la communication et à l'accès étaient fondées.

Il n'était pas nécessaire qu'Optique Laurier dévoile les renseignements personnels du plaignant à l'Ordre des opticiens ou aux fabricants de lunettes pour prouver que les verres fournis au plaignant étaient adéquats. Même si ces organisations pouvaient

formuler des commentaires pertinents, elles auraient pu le faire sans connaître le nom, l'adresse et le numéro de téléphone du plaignant ainsi que les détails du différend. Il n'était pas non plus nécessaire de fournir ces renseignements à l'optométriste indépendant.

Nous avons recommandé qu'Optique Laurier donne à son personnel une formation sur les exigences de la LPRPDE liées à la protection des renseignements personnels des clients.

L'organisation ne nous a pas répondu.

Compte tenu des faits examinés au cours de l'enquête et des questions en suspens, la commissaire à la protection de la vie privée était d'avis que les pratiques de traitement des renseignements personnels d'Optique Laurier dans cette affaire devaient être rendues publiques et elle a exercé son pouvoir discrétionnaire de nommer publiquement l'organisation.

Un garage de changement d'huile rapide scanne le certificat d'immatriculation du véhicule d'un client sans que cela ne soit nécessaire

Le client d'un centre de lubrification et de changement d'huile pour automobiles s'est opposé à l'enregistrement des renseignements personnels se trouvant sur le document d'immatriculation de son véhicule alors qu'il voulait simplement faire une vidange d'huile.

Ayant remis en question cette pratique et posé des questions sur le traitement de ses renseignements personnels sans avoir obtenu de réponse de l'entreprise, il a déposé une plainte au Commissariat.

Le plaignant était un client régulier d'un garage où l'on effectue des vidanges d'huile rapides. Au cours d'une de ses visites, un employé lui a demandé de fournir le certificat d'immatriculation de son véhicule pour en lire le code à barres. Le plaignant s'est demandé pourquoi c'était nécessaire puisque le numéro d'identification du véhicule fournit suffisamment d'information (c.-à-d. la marque, le modèle, l'année, la qualité d'huile et le numéro de filtre) pour faire une vidange d'huile.

Il s'est montré encore plus préoccupé lorsque la société d'assurance automobile de sa province l'a informé que le code à barres du certificat d'immatriculation de sa voiture comprenait également son numéro de permis de conduire.

Il a téléphoné aux bureaux de l'atelier pour demander une explication plus satisfaisante, mais personne n'a rappelé et le responsable de la protection de la vie privée n'a pas répondu à sa demande d'information écrite.

Dans la réponse qu'il a donnée au Commissariat, le propriétaire de l'entreprise a admis que le code d'immatriculation du véhicule comprenait plus de renseignements personnels que le numéro d'identification, mais il a affirmé du même souffle que cela pouvait être utile pour confirmer l'exactitude des renseignements qui se trouvent au dossier du client.

Les clients qui se présentent pour la première doivent aussi fournir leur nom, leur adresse et leur numéro de téléphone, même si ces renseignements ne sont pas nécessaires. Ces derniers sont nécessaires dans le cadre de travaux couverts par une garantie ou de plaintes concernant le service, ou sont demandés à titre préventif dans l'éventualité où les employés découvriraient l'existence d'un problème en travaillant sur le véhicule et où il serait nécessaire de communiquer avec le client.

Même si d'autres renseignements personnels figurent dans le code à barres du certificat d'immatriculation du véhicule (p. ex. les frais d'assurances et d'immatriculation provinciaux, le numéro de permis de conduire), nous avons confirmé que la technologie de lecture du centre de vidanges d'huile permettait seulement de lire le nom et l'adresse du propriétaire enregistré du véhicule, l'année de fabrication, la marque, le modèle, la classe, la couleur et le numéro de plaque.

Bien qu'il ait été prouvé que l'organisation n'avait pas obtenu, en scannant le certificat d'immatriculation du véhicule, de renseignements personnels du client qu'elle ne possédait pas déjà dans ses dossiers, nous avons convenu que les préoccupations du plaignant étaient légitimes; il n'est pas nécessaire de recueillir les renseignements inscrits sur le certificat d'immatriculation d'un véhicule pour faire une vidange d'huile.

Nous avons recommandé que l'entreprise mette fin à sa pratique de demander et de scanner les certificats d'immatriculation des véhicules de ses clients.

Nous avons aussi recommandé que l'entreprise mette en place des politiques et des procédures pour que les personnes puissent communiquer avec un responsable de la protection de la vie privée capable de traiter les demandes de renseignements et les plaintes dans ce domaine.

L'entreprise n'a pas suivi les recommandations du Commissariat et n'a pas répondu à nos appels de suivi.

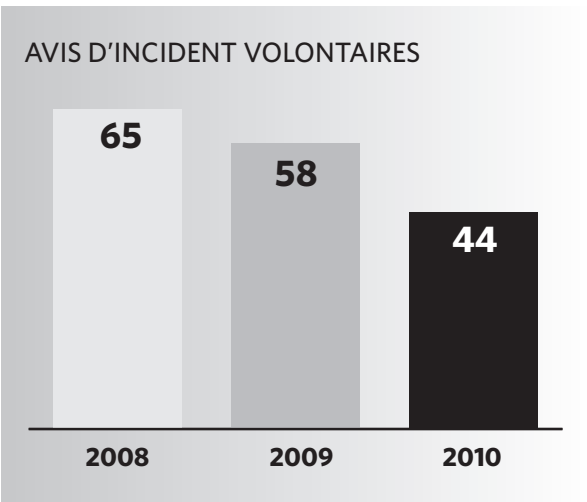
Le Commissariat avait envisagé de porter l'affaire devant la Cour fédérale pour obliger l'entreprise à se conformer à ses obligations en matière de protection des renseignements personnels, mais le plaignant nous a demandé de ne pas poursuivre les procédures. Or, la LPRPDE exige que la commissaire à la protection de la vie privée obtienne le consentement du plaignant avant de présenter une demande d'audience à la Cour.

4.8 Atteinte à la sécurité des renseignements personnels

Le Commissariat invite les organisations à signaler volontairement les atteintes à la protection des données.

En 2010, 44 atteintes à la protection des données dans le secteur privé ont été signalées volontairement. Le nombre d'avis volontaires diminue pour une deuxième année consécutive.

Nous espérons toujours l'adoption de modifications législatives qui obligeraient à signaler les atteintes importantes à la protection des données au Commissariat et aux personnes concernées. Les modifications étaient en cours d'examen au Parlement à la fin de 2010.



Un régime de signalement obligatoire nous donnera une meilleure idée du nombre d'incidents, de leur cause et des mesures à prendre pour atténuer le risque qu'ils se reproduisent.

Le secteur financier semble être celui où l'on signale le plus souvent des atteintes à la protection des données. En 2010, les deux tiers des avis d'incident volontaires (29) provenaient d'institutions financières. Des responsables de la protection de la vie privée de grandes institutions financières du Canada nous ont dit qu'ils avaient consciemment décidé de signaler proactivement les incidents, même si la loi les obligeant à le faire n'a pas encore été adoptée. Nous les félicitons d'avoir fait ce choix.

Le fait que le Commissariat soit informé d'une atteinte et surveille les mesures prises par l'organisation pour remédier à la situation a souvent pour effet de rassurer les personnes concernées et d'empêcher que des plaintes soient déposées au Commissariat à la protection de la vie privée.

Quand le Commissariat reçoit un avis d'incident, il collabore avec le responsable de la protection de la vie privée de l'organisation pour faire en sorte que les mesures nécessaires soient prises et que les personnes touchées reçoivent de l'information pertinente et puissent faire part de leurs préoccupations.

En 2010, plus du tiers (15 sur 44) des avis d'incident reçus portaient sur l'accès non autorisé à des renseignements personnels – souvent par des employés de l'organisation.

Presque autant de cas (14) étaient liés à un vol de renseignements personnels, découlant souvent du vol d'un ordinateur portatif.

EXEMPLES D'AVIS D'INCIDENT

Base de données piratée

La base de données d'un détaillant canadien de vêtements pour enfants a été piratée et les renseignements personnels des clients ont été affichés sur son site Web durant un court moment. Pendant ce temps, un moteur de recherche a mis le site Web en mémoire cache et les renseignements personnels sont devenus interrogeables. Les médias ont appris l'incident et rapporté la nouvelle. En réponse à une demande du Commissariat, l'entreprise a reconnu qu'il y avait eu une atteinte à la sécurité des renseignements personnels. Le détaillant nous a appris qu'il avait essayé en vain de faire en sorte que le moteur de recherche supprime les pages. Un agent de résolution rapide est intervenu et les renseignements ont finalement été retirés.

Préoccupations liées à la fonction « recomposition » d'un téléphone

Le Commissariat a reçu une demande d'un média au sujet des téléphones de deux kiosques de transactions bancaires permettant aux consommateurs de faire des opérations bancaires par téléphone. Le média soutenait qu'à l'aide du bouton de recomposition des téléphones, on pouvait obtenir des renseignements permettant d'accéder aux comptes des clients, d'obtenir d'autres renseignements et même de faire des transactions. Quand le Commissariat a communiqué avec la banque, celle-ci a affirmé que, d'après les tests effectués sur les téléphones, il est impossible d'appuyer sur recomposition et d'obtenir les renseignements nécessaires pour accéder aux comptes d'autrui. Toutefois, à titre de précaution, la banque a remplacé les deux téléphones par de nouveaux appareils qui n'étaient pas dotés d'un bouton de recomposition. La banque s'est aussi engagée à remplacer les téléphones de toutes ses succursales.

CHAPITRE 5

Sensibiliser les Canadiennes et les Canadiens

Notre rôle consiste en grande partie à informer les Canadiennes et les Canadiens de leur droit à la vie privée et à aider les organisations à apprendre comment mieux remplir leurs obligations en vertu de la LPRPDE.

Nous vivons à une époque où des gens vivent leur vie comme des vedettes de téléréalité, partageant avec enthousiasme leurs pensées et leurs images les plus intimes sur Internet.

Même ceux qui ne sont pas des exhibitionnistes numériques fournissent énormément de renseignements sur eux-mêmes. En employant des cartes de fidélité, par exemple, ils échangent activement des renseignements personnels contre des rabais en magasin ou d'autres cadeaux publicitaires.

Et nous parlons ici de ce que les gens font consciemment. Il y a par ailleurs une réalité inconnue de la plupart des internautes, soit celle de la collecte massive de données, qui se produit lors de la consultation de sites Web ou d'achats en ligne.

Toutes ces activités ont de profondes répercussions sur la vie privée, mais il n'est pas toujours facile de comprendre comment ces pièces s'imbriquent les unes dans les autres.

Cela ne signifie pourtant pas que les gens ne se préoccupent pas de leur vie privée; nos enquêtes démontrent qu'au contraire, ils le sont.

C'est pourquoi le Commissariat consacre beaucoup d'efforts à la sensibilisation du public. Nous parlons aux gens de leur droit à la vie privée, de la façon dont ce droit est mis à l'épreuve et parfois même compromis et de ce qu'ils peuvent faire pour remédier à la situation.

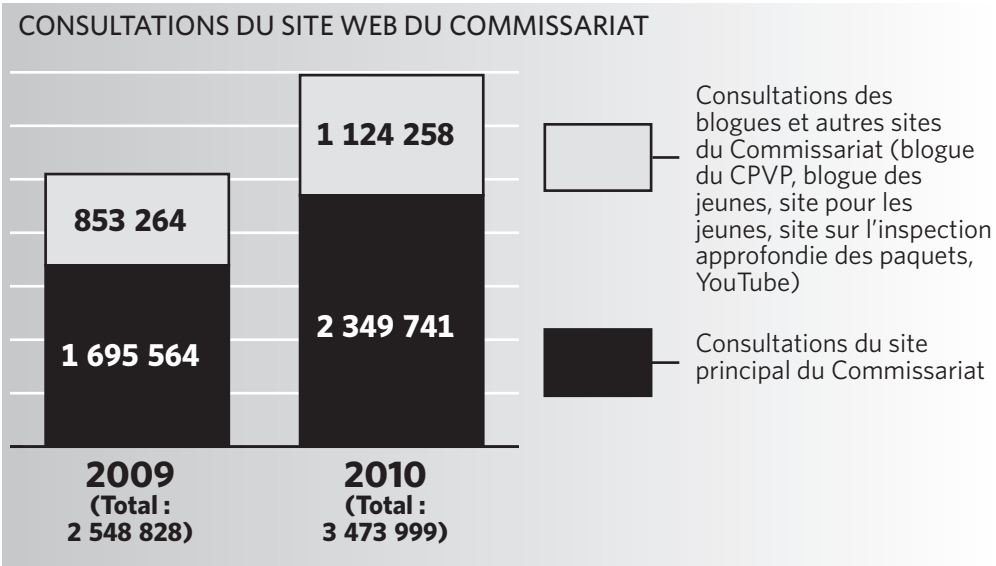
Nous nous adressons également aux entreprises pour les sensibiliser à l'égard de leurs obligations en vertu de la LPRPDE et leur expliquer comment le mieux protéger les renseignements personnels des Canadiennes et des Canadiens.

L'un des principaux moyens utilisés pour ce faire est la participation à des conférences et autres activités, où nous faisons des présentations et présentons des expositions. Nous sommes invités à parler dans le cadre de conférences de haut niveau dans le monde entier. En 2010, nous avons accepté environ les trois quarts des invitations que nous avons reçues. La commissaire, les commissaires adjointes et d'autres membres du personnel du Commissariat ont fait 150 discours et présentations.

Nous estimons que les médias sont un autre moyen très efficace de sensibiliser les Canadiennes et les Canadiens, ainsi que les organisations. Au cours des dernières années, nous avons constaté que les médias s'intéressaient de plus en plus aux questions relatives à la protection de la vie privée, notamment celles touchant le cyberespace. Le Commissariat accepte autant de demandes d'entrevue qu'il le peut (il en a donné 250 en 2010 seulement) pour passer son message concernant d'importants enjeux en matière de protection de la vie privée.

Pour ce qui est de la protection de la vie privée en ligne, nous mettons l'accent sur la culture numérique, en aidant les personnes à acquérir les compétences et les connaissances en matière numérique dont elles ont besoin pour protéger leurs renseignements personnels et en veillant à ce que les entreprises fournissent à leurs clients les renseignements et instruments dont ils ont besoin pour faire des choix éclairés en matière de protection de la vie privée.

Le taux de consultation de nos sites Web de plus en plus nombreux (site principal, blogue, site pour les jeunes, blogue des jeunes, site sur l'inspection approfondie des paquets, YouTube) a augmenté de façon spectaculaire. De 2009 à 2010 seulement, nous avons enregistré une augmentation des consultations de 36 %.



Au cours des trois dernières années, le Commissariat s'est servi des réseaux sociaux pour sensibiliser le public aux enjeux associés à la protection de la vie privée.

Nous avons lancé le blogue du Commissariat en 2007 et le blogue des jeunes en 2008. Nous avons également ouvert un compte sur Twitter en 2010 pour y communiquer des nouvelles et des renseignements et y échanger avec des intervenants du milieu de la protection de la vie privée et d'autres personnes intéressées. À la fin de l'année, nous avions envoyé plus de 700 « tweets » et attiré près de 2 000 abonnés.

Au printemps, nous avons employé Twitter pour stimuler la discussion au cours de nos consultations sur la protection de la vie privée des consommateurs. Nous avons « tweeté en direct » et invité les participants à en faire autant. Nous avons répondu à des questions de l'auditoire et des personnes écoutant la webdiffusion, par l'intermédiaire de Twitter.

Nos publications imprimées restent également très en demande. Nous en avons distribué 15 478 en 2010. Il s'agissait – en plus des dépliants, documents d'orientation et fiches d'information – de nos guides à l'intention des entreprises et des personnes, du livret intitulé *La protection de la vie privée dans une société en évolution* et de nos rapports annuels.

Nous avons également recours à des méthodes novatrices pour faire passer notre message. Par exemple, nous avons demandé à un bédéiste de créer des illustrations pour véhiculer notre message sur la protection de la vie privée de façon humoristique. Ces illustrations ont servi dans le cadre de présentations et ont été imprimées sur

des affiches, des cartes postales et notre calendrier.

Voici un aperçu de quelques-unes de nos principales activités de sensibilisation en 2010.

5.1 Sensibilisation des entreprises

BUREAU DE TORONTO

À l'automne 2010, le Commissariat a inauguré un nouveau bureau à Toronto. La présence du Commissariat à Toronto permet de stimuler les relations avec les entreprises, les associations de l'industrie, les universités et d'autres intervenants de la région. Nous pouvons, par exemple, mieux cibler et rendre plus efficaces les mesures que nous prenons pour conseiller et sensibiliser les intéressés aux principaux enjeux en matière de vie privée.

Un grand nombre de nos enquêtes sont menées à partir du bureau de Toronto. Une analyse des plaintes relatives à la LPRPDE reçues pendant la période s'échelonnant de janvier 2008 et à la mi-mai 2010 a démontré que 44,5 % des organisations intimées, ou leur siège social, étaient situés dans la région du Grand Toronto.

Nous avons bâti des réseaux de collaboration pour appuyer nos activités d'éducation et de sensibilisation actuelles et à venir dans la région. Nous avons également organisé une série de séances d'information à l'intention d'entreprises et d'intervenants du milieu de la protection de la vie privée du Grand Toronto. Dans le cadre de ces séances, nous avons abordé des questions systémiques, expliqué les obligations de chacun en matière de protection de la vie privée et mis en valeur les instruments et produits d'information du Commissariat.

Aux fins de la planification de l'ouverture du bureau de Toronto, nous avons fait enquête auprès de petites et grandes entreprises et constaté qu'une majorité d'entre elles étaient en faveur du projet, qui constitue, selon elles, un moyen de promouvoir le discours sur la protection de la vie privée et d'informer les entreprises du secteur privé – notamment les petites et moyennes entreprises – de la réglementation applicable à la protection de la vie privée et de leurs obligations en la matière.

OUTIL EN LIGNE POUR LES PETITES ENTREPRISES

Le Commissariat a souligné la Semaine des petites entreprises en octobre 2010 en lançant un outil en ligne perfectionné, destiné à aider les entreprises à protéger la vie privée de leurs clients. Cet outil leur permet de déterminer le volume d'information dont elles ont besoin sur leurs clients et les moyens de protéger ces renseignements.

L'outil en ligne de protection de la vie privée pour les petites entreprises propose une évaluation interactive destinée précisément aux entreprises. Il guide l'utilisateur pas à pas dans le dédale de renseignements dont il a besoin pour respecter la réglementation en matière de protection de la vie privée et offrir aux clients une protection conforme à leurs attentes.

L'outil est facile à utiliser, et l'évaluation peut être effectuée en une demi-heure environ. Au terme de l'exercice, les propriétaires d'entreprise disposent des éléments suivants :

- une vérification des pratiques de traitement de l'information de l'entreprise;
- des dispositions en matière de consentement conçues spécifiquement pour leur entreprise;
- un plan de sécurité pour la protection des renseignements personnels qui leur sont confiés;
- un modèle de dépliant sur la protection de la vie privée destiné à leurs clients;
- une évaluation de leurs besoins en matière de formation.

LE MILIEU DE LA TI

Grâce à l'arrivée de deux nouveaux analystes de recherche en informatique, le Commissariat a été en mesure d'intensifier ses activités de sensibilisation à l'intention du milieu de la technologie de l'information.

Au cours de l'année 2010, ces analystes ont été invités à parler de la technologie et des enjeux liés à la protection de la vie privée à des étudiants des universités de Waterloo, Harvard, Columbia, Princeton et de la Pennsylvanie.

Ils ont également présenté des exposés à d'importantes conférences sur la sécurité et la protection de la vie privée, notamment au congrès sur la vie privée et la sécurité de l'information organisé par Reboot Communications, au sommet sur la cybercriminalité

au Canada de l'Alliance nationale d'intervention judiciaire et de formation contre la cybercriminalité et à la conférence du Digital Crimes Consortium.

5.2 Sensibilisation des personnes

PROTECTION DE LA VIE PRIVÉE DES JEUNES

Les enfants sont initiés à Internet de plus en plus tôt et ils y passent de plus en plus de temps. Ils sont également parmi les premiers à adopter les nouvelles technologies, avant même qu'on ait pu repérer les risques pour la vie privée. Le Commissariat adapte ses programmes d'éducation et de sensibilisation sur la protection de la vie privée des jeunes en fonction des nouveaux enjeux auxquels ces derniers sont confrontés sur Internet.

Pour mieux circonscrire les connaissances qui font défaut aux jeunes et mieux comprendre de quelle manière ils préfèrent obtenir de l'information, nous avons mis sur pied un groupe consultatif d'adolescents provenant de toutes les régions du pays. Leurs points de vue et opinions se sont révélés très utiles pour orienter nos initiatives en matière de protection de la vie privée dans l'univers numérique.

Depuis 2009, nos employés font des présentations dans les écoles sur le réseautage social et les risques qui y sont associés pour la vie privée. Ces présentations sont devenues très populaires au cours de la dernière année. En 2010, nous en avons fait 134 devant plus de 21 000 élèves de la 4e à la 12e année, mais aussi des parents, des enseignants et des policiers œuvrant dans les écoles.

Nous avons également proposé des versions modifiées de la présentation à des auditoires spécialisés : adolescents autistes et accusant un retard de développement, la plupart sur Facebook. Nous nous sommes également adressés à des adolescents inscrits dans des écoles secondaires alternatives.

Les réactions que nous avons obtenues donnent à penser que les adultes et les jeunes ont apprécié l'information et l'expertise que nous leur avons communiquées. Le caractère interactif des présentations a également incité les jeunes à participer et consolidé notre propre compréhension de leur comportement en ligne.

Le site vie privée des jeunes continue d'être une source de renseignements et de conseils pour les parents, les enseignants et les jeunes désireux de protéger leur vie privée sur Internet. En 2010, le Commissariat a affiché des messages sur le blogue du site – au sujet du géomarquage, de la citoyenneté numérique, de l'hameçonnage et des applications

tierces dans les sites de réseautage social – dans le but d'intéresser et d'informer les enfants et les adolescents.

Pour la deuxième année consécutive, nous avons organisé un concours de vidéos pour les élèves. L'enthousiasme suscité par le concours s'est concrétisé par plus de 100 propositions provenant de partout au pays. À l'occasion d'une activité organisée de concert avec le forum jeunesse Rencontres du Canada, les vidéos gagnantes ont été choisies par 120 jeunes de toutes les régions du pays.

PrivacyCampTO

En juin 2010, le Commissariat a appuyé la première conférence PrivacyCampTO sur la vie privée à l'ère numérique. La rencontre d'une journée, qui s'est déroulée à l'Université Ryerson de Toronto, a été le fruit d'une collaboration dans la mesure où ce sont les participants qui ont décidé de l'ordre du jour au début de la conférence. Cela a donné lieu à des échanges animés entre les chercheurs, les universitaires et les militants.

Les participants ont discuté des risques pour la vie privée associés aux réseaux sociaux. Il y a également eu du « speed geeking » (expression inspirée du speed dating), qui consiste à faire des présentations dans de très courtes périodes de temps. Les présentations ont traité de moyens techniques pour renforcer la protection de la vie privée, par exemple des outils de chiffrement et des conseils pratiques sur la façon de supprimer définitivement des profils dans les réseaux sociaux.

CONFÉRENCIERS

En 2010, le Commissariat a lancé une série de discussions informelles intitulée « Le point sur la vie privée », dont le but est de fournir une tribune à des chercheurs qui mènent des travaux intéressants dans le domaine de la protection de la vie privée.

Lors d'une première activité, en décembre dernier, nous avons accueilli le radiodiffuseur et stratège d'Internet Jesse Hirsh et le chercheur en matière de vie privée Christopher Soghoian. Leurs réflexions stimulantes sur l'avenir de la vie privée ont attiré plus de 60 personnes. Le tout a été filmé sur vidéo et affiché sur YouTube (où nous avons également affiché d'autres vidéos).

Nous avons l'intention de tenir d'autres activités avec divers conférenciers dans le but de discuter d'enjeux actuels en matière de protection de la vie privée avec des auditoires présents sur place.

5.3 Sensibilisation partout au Canada

À l'occasion de la rencontre de septembre 2010 à Whitehorse, les commissaires à la protection de la vie privée des gouvernements fédéral, provinciaux et territoriaux ont décidé de travailler de concert pour sensibiliser les Canadiennes et les Canadiens aux enjeux associés à la protection de la vie privée.

Le Commissariat souhaite collaborer avec les commissaires provinciaux et territoriaux en vue de l'élaboration de programmes de sensibilisation efficaces et durables. Nous mettons l'accent sur la sensibilisation des petites entreprises, à l'égard des enjeux liés à la protection de la vie privée et aux moyens de la protéger et sur la culture numérique des Canadiennes et des Canadiens, notamment celle des jeunes.

Nous travaillons également avec nos homologues provinciaux et territoriaux à l'élaboration de programmes localisés et ciblés dans leur région.

Dans les provinces de l'Atlantique, un accord d'échange de deux ans conclu avec un conseiller principal en recherche et sensibilisation de la région est venu à échéance en 2010. Installé à Saint-John (Terre-Neuve), notre représentant a fait, dans toute la région, plus de 70 présentations à l'intention de jeunes, de petites entreprises, d'organismes communautaires, d'associations professionnelles, de chambres de commerce et de sociétés d'aide aux entreprises.

5.4 Programme des contributions

Pour la troisième année consécutive, le Programme des contributions du Commissariat a permis de financer des projets d'éducation et de sensibilisation du public, ainsi que la recherche dans le secteur de la protection de la vie privée.

En 2010, par exemple, notre aide a permis à Option consommateurs d'organiser des ateliers et d'élaborer un guide pour sensibiliser les consommateurs à la collecte et à l'utilisation des renseignements personnels dans les rapports de solvabilité.

Toujours grâce au financement du programme des contributions, un autre groupe, l'Union des consommateurs, a organisé une conférence de deux jours sur les difficultés et les possibilités pour les consommateurs à l'ère numérique. La conférence a eu lieu à Montréal en mars 2011.

5.5 Allocutions

Les allocutions représentent un autre volet important de notre programme de sensibilisation. Nous faisons des présentations sur une foule de sujets liés à la vie privée à l'intention de groupes d'entreprises, dans le cadre de conférences et dans les écoles et les universités.

En 2010, nous avons participé à 150 activités publiques partout au pays. La commissaire, les commissaires adjointes et des membres de notre personnel se sont exprimés dans le cadre de conférences destinées à des spécialistes de divers domaines. Nous étions présents au Sommet canadien sur la protection de la vie privée 2010, organisé par l'International Association of Privacy Professionals, à la Conférence mondiale 2010 sur le droit de la technologie, organisée par ITechLaw, à la 11e Conférence annuelle sur la protection des renseignements personnels et la sécurité et au SC Magazine World Congress Canada.

CHAPITRE 6

Devant les tribunaux

Du point de vue de la jurisprudence, la LPRPDE est une loi relativement récente et son interprétation continue de soulever de nouvelles questions d'ordre légal. En 2010, les tribunaux ont eu maille à partir avec, entre autres choses, l'étendue du pouvoir de la commissaire, la définition du terme « activité commerciale » et la question des dommages-intérêts suite à une contravention à la LPRPDE.

Le Commissariat a continué de se présenter devant les tribunaux en vue de leur fournir une orientation à l'égard du traitement des questions susmentionnées et de l'application des obligations que les organisations sont tenues de respecter aux termes de la loi.

En vertu de la LPRPDE, un plaignant peut, après avoir reçu un rapport du Commissariat et dans des circonstances précises, demander une audience à la Cour fédérale pour toute question évoquée dans sa plainte ou dans le rapport de la commissaire (article 14 de la LPRPDE).

La LPRPDE habilite la commissaire à demander directement, avec le consentement du plaignant, une audience à la Cour fédérale concernant cette même affaire (article 15 de la LPRPDE). Aux termes de la loi, la commissaire peut également comparaître devant la Cour fédérale au nom d'un plaignant ayant demandé une audience ou, avec l'autorisation de la Cour, comparaître comme partie à toute audience demandée par un plaignant (article 15 de la LPRPDE).

Cette année, la commissaire a fait de nouvelles demandes en vertu de la loi, et certaines demandes passées émanant de la commissaire ont fait l'objet de décisions. Une affaire a également fait l'objet d'un règlement négocié.

La commissaire à la protection de la vie privée intente régulièrement des poursuites lorsqu'une organisation refuse d'adopter ses recommandations à la suite de plaintes jugées fondées. Nous avons constaté que cela entraîne un degré élevé de conformité aux recommandations.

Conformément à l'esprit de notre mandat, nous avons respecté la vie privée des plaignants en ne mentionnant pas leur nom dans ce rapport.

6.1 Demandes déposées par la commissaire (article 15 de la LPRPDE)

Commissaire à la protection de la vie privée du Canada c. Canad Corporation of Manitoba Ltd., faisant affaire sous le nom de Canad Inns
Numéro de dossier de la Cour fédérale : T-586-08

En 2010, nous avons obtenu un règlement négocié dans une poursuite intentée par la commissaire à la suite d'une enquête sur la collecte de renseignements personnels concernant les clients d'un bar au moyen d'un appareil qui recueillait et conservait les renseignements personnels figurant au recto d'une pièce d'identité comme un permis de conduire.

Comme nous l'avions indiqué dans le rapport annuel de 2009, l'enquête a été déclenchée par la plainte d'une cliente de Canad Inns qui s'était opposée à ce que les renseignements inscrits sur son permis de conduire soient enregistrés.

Le Commissariat comprenait bien que Canad Inns avait besoin de vérifier l'âge de ses clients et de veiller à la sécurité de ses boîtes de nuit. Pour garantir la sécurité de ses clients, outre les appareils d'enregistrement de l'identité, l'entreprise employait un système de vidéosurveillance, des détecteurs de métal, des fouilles sommaires, du personnel de sécurité et des listes de personnes interdites d'accès.

Après enquête, nous avons constaté que les appareils d'enregistrement de l'identité recueillaient plus de renseignements que Canad Inns n'en avait besoin pour vérifier l'âge des clients et garantir la sécurité. Nous avons donc recommandé à l'entreprise de cesser de recueillir et de conserver des renseignements personnels de cette façon et de supprimer les renseignements personnels de ses clients de ses unités de stockage des données d'identification.

Canad Inns s'est dit en désaccord avec ces recommandations. Avec le consentement de la plaignante, nous avons demandé une audience à la Cour fédérale afin de les faire respecter.

À la suite d'une médiation ordonnée par la Cour en 2009, celle-ci a accordé à Canad Inns un certain délai pour déterminer les moyens par lesquels elle pourrait limiter les renseignements personnels qu'elle recueille.

En juillet 2010, nous avons conclu avec Canad Corporation of Manitoba Ltd. (Canad Inns) un règlement négocié en vertu duquel l'entreprise s'est engagée à ce qui suit :

- cesser de recueillir des renseignements personnels dans ses boîtes de nuit à l'aide d'appareils d'enregistrement de l'identité;
- détruire les renseignements personnels recueillis à l'aide de ces appareils;
- limiter le volume de renseignements personnels inscrits dans sa liste de personnes interdites d'accès et veiller à ce que ces renseignements soient correctement protégés.

Le Commissariat est heureux que Canad Inns ait accepté de prendre des mesures pour garantir que le droit de ses clients à la protection de leur vie privée soit respecté.

Ainsi, l'entreprise ne recueillera plus que certains renseignements personnels (nom, date de naissance et photo) et ne les conservera que pour une durée de 24 heures.

Une approche semblable a été adoptée en Colombie-Britannique et en Alberta, où les commissaires à la protection de la vie privée ont fait enquête sur des cas similaires.

Commissaire à la protection de la vie privée c. Air Canada
Numéro de dossier de la Cour fédérale : T-143-09

Par suite d'un incident survenu lors d'un vol court-courrier, une personne a demandé à avoir accès à ses renseignements personnels conservés par Air Canada. La compagnie aérienne a refusé de fournir les renseignements, invoquant le secret professionnel de l'avocat.

La personne a porté plainte auprès du Commissariat. Nous n'avons pu régler l'affaire dans le cadre de notre enquête, car Air Canada refusait de fournir au Commissariat suffisamment de détails justifiant sa revendication du secret professionnel de l'avocat. Nous avions demandé qu'Air Canada fournisse une déclaration sous serment pour étayer cette revendication.

Air Canada estimait que le Commissariat n'avait pas le pouvoir d'enquêter sur les revendications du secret professionnel liant l'avocat à son client conformément à la décision de la Cour suprême du Canada dans l'affaire *Canada (commissaire à la protection de la vie privée) c. Blood Tribe Department of Health*.

En janvier 2009, nous avons déposé une demande d'audience pour obtenir, entre autres, une déclaration confirmant que la commissaire à la protection de la vie privée était

habilitée, en vertu du paragraphe 12(1) de la LPRDPE, à enquêter sur des plaintes relatives au refus d'Air Canada de fournir l'accès aux renseignements personnels fondé sur une revendication au secret professionnel liant l'avocat à son client (aux termes de l'alinéa 9(3)*a*) de la LPRPDE), et à exiger la production d'une preuve par affidavit pour étayer sa revendication de privilège.

L'affaire a été entendue en mars 2010, et la Cour fédérale a rendu sa décision le 20 avril 2010.

En ce qui concerne le pouvoir de la commissaire de demander à Air Canada de justifier sa revendication de privilège par voie d'affidavit, le juge Harrington s'est appuyé sur la décision de la Cour suprême dans *Canada (commissaire à la protection de la vie privée) c. Blood Tribe Department of Health,* [2008] 2 R.C.S. 574, qui lui a permis de conclure que la commissaire « ne pouvait pas décider des mesures nécessaires qu'Air Canada devait suivre pour prouver que les documents étaient réellement protégés par le secret professionnel ».

Le juge Harrington a conclu que la compétence pour trancher la question du secret professionnel de l'avocat revenait à la Cour fédérale et non à la commissaire. Il s'est dit d'avis qu'Air Canada avait fourni suffisamment de raisons pour étayer sa revendication du secret professionnel de l'avocat. De plus, le juge Harrington a souligné que, si la commissaire n'était pas d'accord avec la revendication de privilège d'Air Canada, elle avait la possibilité de porter l'affaire devant la Cour fédérale.

Au sujet de la protection par le secret professionnel des documents retenus par Air Canada, le juge Harrington a conclu que ceux-ci n'étaient pas tous protégés, contrairement à ce que prétendait Air Canada. Le juge Harrington a estimé qu'un rapport – un document de routine résumant l'affaire – préparé par un représentant du service à la clientèle d'Air Canada n'était pas protégé et a ordonné à la compagnie de fournir au plaignant une copie de ce rapport.

Commissaire à la protection de la vie privée c. Sobeys Inc.
Numéro de dossier de la Cour fédérale : T-243-10

La commissaire à la protection de la vie privée s'est adressée à la Cour fédérale en vertu de l'article 15 de la LPRPDE à la suite d'une plainte concernant la pratique de Sobeys de demander à tous les clients qui achètent des produits du tabac de présenter une pièce d'identité quel que soit leur âge apparent.

En cours d'enquête, Sobeys a expliqué qu'elle avait adopté cette politique en Ontario afin de respecter les dispositions de la *Loi favorisant un Ontario sans fumée*. Cette loi interdit de vendre des produits du tabac aux personnes de moins de 19 ans et exige que

les détaillants demandent une pièce d'identité aux personnes qui semblent avoir moins de 25 ans.

Le Commissariat a recommandé à Sobeys d'adopter d'autres procédures n'exigeant pas la production d'une pièce d'identité lorsque les clients ont manifestement plus de 25 ans. Le Commissariat a par la suite déposé une demande auprès de la Cour fédérale réclamant une ordonnance selon laquelle Sobeys serait tenue de se conformer à sa recommandation.

À la suite des discussions ayant eu cours entre les parties, Sobeys a modifié sa politique sur les ventes de tabac en Ontario de sorte que les personnes qui ont visiblement l'âge légal pour acheter des produits du tabac seront, dans les circonstances appropriées, exemptées de l'exigence de présenter une pièce d'identité. Sobeys avisera ses clients en Ontario, par moyen d'un message sur son site Web public, que ceux-ci peuvent faire part de toute préoccupation relative aux exigences d'identification de la politique de l'entreprise au gérant du magasin. La commissaire a donc décidé qu'il n'était pas nécessaire de procéder avec sa demande.

Commissaire à la protection de la vie privée c. Association of American Medical Colleges
Numéro de dossier de la Cour fédérale : T-1275-10

La commissaire à la protection de la vie privée a demandé une audience à la Cour fédérale en vertu de l'article 15 de la LPRPDE en raison du refus de l'Association of American Medical Colleges (AAMC) de mettre un terme à la collecte de renseignements biométriques confidentiels (empreintes digitales numériques, photographie numérique et renseignements sur le permis de conduire) sur les candidats au Medical College Admissions Test (MCAT).

L'AAMC recueille ces renseignements pour garantir l'intégrité du MCAT et en raison d'allégations de fraude aux États-Unis et au Canada.

L'AAMC, par l'entremise d'un tiers, recueille des empreintes digitales numériques et d'autres renseignements personnels sur les candidats au MCAT dans les centres d'examen. Les empreintes digitales sont converties en modèle numérique, mais les images sont conservées au cas où le modèle deviendrait corrompu.

Notre enquête portait sur la communication des motifs, la collecte, la conservation et les mesures de sécurité.

Compte tenu des renseignements fournis en cours d'enquête, la commissaire a estimé qu'il existait des moyens portant moins atteinte à la vie privée de répondre aux besoins de l'AAMC en l'espèce.

En réponse au rapport de conclusions d'enquête préliminaire du Commissariat, l'AAMC a déclaré qu'elle réviserait le libellé de l'avis et du consentement en fonction de modifications à venir au sujet de l'utilisation des renseignements personnels. Elle a cependant ajouté qu'elle continuerait de recueillir les empreintes digitales des candidats et de scanner leur permis de conduire et leur photographie.

Le Commissariat a donc conclu que la plainte était fondée et résolue sur le plan de la communication des motifs, mais qu'elle restait fondée sur le plan de la collecte de renseignements.

En août 2010, la commissaire a déposé un avis de requête à la Cour fédérale pour lui demander à titre de redressement une ordonnance enjoignant à l'AAMC de trouver des moyens moins envahissants sur le plan de la protection de la vie privée de garantir l'intégrité de cet examen aux enjeux importants.

Au moment de la rédaction du présent rapport, les parties ont déposé leurs affidavits et leurs pièces documentaires à la Cour.

Commissaire à la protection de la vie privée c. Autorité aéroportuaire du Grand Toronto
Numéro de dossier de la Cour fédérale : T-1885-10

La commissaire à la protection de la vie privée a présenté cette demande en vertu de l'article 15 de la LPRPDE. La plainte concerne la collecte indue de renseignements personnels par une employée de l'Autorité aéroportuaire du Grand Toronto (GTAA) et le refus de la GTAA d'octroyer au plaignant l'accès aux renseignements personnels le concernant qui se trouvent sous le contrôle celle-ci.

Le plaignant allègue notamment que son ex-épouse, une employée de la GTAA, a fait une utilisation inappropriée de l'équipement de la GTAA pour recueillir des photographies de lui et de sa famille alors que ceux-ci se trouvaient à l'aéroport international Pearson de Toronto. Le plaignant a également demandé à la GTAA l'accès à ses renseignements personnels. Insatisfait de la manière dont la GTAA a mené l'enquête et sa demande d'accès, le plaignant a porté plainte auprès du Commissariat. Nous avons jugé que la plainte était fondée et avons fait une demande en vertu de l'article 15 de la LPRPDE.

La demande adressée à la Cour soulève, entre autres, la question de savoir si la GTAA a omis de respecter ses obligations en vertu de la LPRPDE lorsque son employée a recueilli et utilisé des renseignements personnels sur le plaignant à l'insu de celui-ci et sans son consentement. Elle soulève également la question de savoir si la GTAA a permis au plaignant d'avoir accès aux renseignements personnels le concernant qu'elle avait en sa possession.

Le Commissariat demande par ailleurs des dommages-intérêts en vertu de l'alinéa 16*c*) de la LPRPDE en raison des faits entourant la collecte de renseignements personnels en l'espèce.

Au moment de la rédaction de ce rapport, l'affaire était toujours en instance devant la Cour fédérale.

Le plaignant, qui est représenté, a également présenté une demande en vertu de l'article 14 de la LPRPDE. Il demandait diverses réparations, dont des dommages-intérêts.

Nota : Pour de plus amples détails sur cette enquête, voir le chapitre 4.

6.2 Demandes de contrôle judiciaire présentées en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*

State Farm c. Commissaire à la protection de la vie privée du Canada et procureur général du Canada
Numéro de dossier de la Cour fédérale : T-604-09

Cette affaire découle d'une demande de contrôle judiciaire déposée par la State Farm Mutual Automobile Insurance Company (State Farm), en vertu de laquelle celle-ci conteste la compétence de la commissaire à la protection de la vie privée du Canada à faire enquête sur une plainte déposée contre l'entreprise en vertu de la LPRPDE.

Dans sa demande de contrôle judiciaire, State Farm demandait diverses réparations, dont une déclaration selon laquelle State Farm ne mène pas d'activités commerciales lorsqu'elle recueille, utilise et communique des renseignements personnels en vue de défendre ses assurés contre un litige entamé par le plaignant et que, si tel était le cas dans ce contexte, la LPRPDE n'est pas valide sur le plan constitutionnel.

L'affaire a été entendue en avril 2010, et le juge Mainville de la Cour fédérale a rendu sa décision en juillet 2010.

En l'espèce, une personne (ci-après « G. ») a été impliquée dans un accident de voiture avec une autre personne (ci-après « V. »), laquelle était assurée par State Farm. Après l'accident, G. a intenté une poursuite contre V. pour les blessures et pertes découlant de l'accident.

State Farm a chargé un enquêteur de faire la lumière sur les réclamations de G. Celui-ci a par la suite demandé à State Farm de lui communiquer les renseignements personnels relatifs à l'enquête, notamment des copies des bandes de surveillance ou de rapports le

concernant. State Farm a refusé, et G. a déposé une plainte au Commissariat pour refus d'accès. Il s'est également plaint que State Farm avait communiqué ses renseignements personnels sans son consentement et ne les avait pas protégés.

Le Commissariat a fait enquête et cherché à obtenir des renseignements auprès de State Farm, qui a refusé de collaborer à l'enquête ou de fournir des renseignements. L'entreprise a affirmé qu'elle n'avait pas recueilli, utilisé ou communiqué de renseignements personnels concernant G. dans le cadre d'activités commerciales et que, par conséquent, le Commissariat n'était pas habilité à faire enquête sur les plaintes de G.

State Farm a fait une demande de contrôle judiciaire pour contester la compétence de la commissaire à la protection de la vie privée à faire enquête et a désigné la commissaire et le procureur général du Canada comme défendeurs.

La Cour a été saisie notamment des questions suivantes :

- La collecte d'éléments de preuve par un assureur représentant l'un de ses assurés dans le cadre de la défense d'une action en responsabilité délictuelle d'un tiers constitue-t-elle une « activité commerciale » au sens de la LPRPDE?

- Dans l'affirmative, l'application de la LPRPDE à des organisations qui ne sont pas des entreprises fédérales outrepasse-t-elle le pouvoir constitutionnel du Parlement?

Concernant la première question, le juge Mainville a statué que la collecte d'éléments de preuve sur un plaignant par une personne qui se trouve à être le défendeur dans une action en responsabilité délictuelle intentée par ce plaignant ne constitue pas une activité commerciale au sens de la LPRPDE parce qu'aucun caractère commercial n'est associé à cette activité.

Quant à savoir s'il y a activité commerciale aux fins de la LPRPDE, le juge Mainville a estimé que, si l'activité ou le comportement n'est pas une activité commerciale telle que l'envisage la LPRPDE, cette activité ou ce comportement est exempté de l'application de la loi, même si une personne confie à des tiers le soin de s'en charger. Le juge Mainville a conclu que la caractérisation première de l'activité ou du comportement est le facteur prépondérant dans l'évaluation de son caractère commercial.

Appliquant son analyse en l'espèce, le juge Mainville a conclu que « la LPRPDE ne s'applique pas aux rapports d'enquête ni aux documents et bandes vidéo connexes qui concernent [G.] et qui ont été établis par la State Farm ou ses avocats, ou en leur nom, pour assurer la défense de [V.] dans l'action en responsabilité civile engagée […] par G. ».

Le juge Mainville a ainsi conclu que la commissaire était habilitée à faire enquête en l'occurrence. Il a souligné par ailleurs qu'il doit « néanmoins exister des mécanismes permettant de tester l'authenticité de l'exclusion ou de la non-application qui est invoquée».

Il a cependant ajouté que, lorsque l'organisation sous enquête invoque le secret professionnel de l'avocat ou le privilège relatif au litige, le pouvoir d'enquête de la commissaire à la protection de la vie privée est limité à cet égard. Il a également rappelé que la commissaire pouvait envisager deux autres avenues : soit renvoyer la question à la Cour fédérale, soit publier un rapport et adresser une demande de réparation à la Cour fédérale en vertu de l'article 15 de la LPRPDE.

Ayant conclu que l'activité en question n'était pas de nature commerciale, le juge Mainville n'a pas abordé les questions d'ordre constitutionnel soulevées par State Farm.

CHAPITRE 7

Lois provinciales et territoriales essentiellement similaires à la loi fédérale

En vertu de l'alinéa 26(2)*b*) de la LPRPDE, le gouverneur en conseil peut exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la LPRPDE à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels dans une province dotée d'une loi essentiellement similaire à la LPRPDE.

Selon le paragraphe 25(1) de la LPRPDE, le Commissariat doit remettre tous les ans au Parlement un rapport sur « la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la loi fédérale.

Dans les rapports annuels antérieurs, nous avons rendu compte des lois du Québec, de l'Ontario (pour les renseignements personnels sur la santé), de l'Alberta et de la Colombie-Britannique, qui ont été déclarées essentiellement similaires.

Selon Industrie Canada, pour être reconnue comme étant essentiellement similaire, une loi provinciale ou territoriale doit :

- inclure les dix principes énoncés à l'annexe 1 de la LPRPDE;
- prévoir un mécanisme de surveillance et de recours indépendant et efficace comprenant le pouvoir d'enquêter;
- restreindre la collecte, l'utilisation et la communication de renseignements personnels à des fins appropriées ou légitimes.

La *Personal Health Information Act* (PHIA) de Terre-Neuve-et-Labrador a reçu la sanction royale le 4 juin 2008. Elle est censée entrer en vigueur en 2011.

La *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (LAPRPS) du Nouveau-Brunswick a reçu la sanction royale le 19 juin 2009. Elle est entrée en vigueur le 1er septembre 2010.

La *Scotia's Personal Health Information Act* (PHIA) a reçu la sanction royale le 10 décembre 2010.

À la demande d'Industrie Canada, nous avons examiné les lois de Terre-Neuve-et-Labrador et du Nouveau-Brunswick et formulé des commentaires sur leur degré de similitude avec la LPRPDE. Au moment de la rédaction du présent rapport, nous n'avons pas reçu de demande d'examen de la loi adoptée par la Nouvelle-Écosse. Une proposition visant la reconnaissance de la similarité de la LAPRPS et de la LPRPDE a été publiée dans la *Gazette du Canada* le 12 mars 2011. Une loi ne peut être déclarée essentiellement similaire avant son entrée en vigueur.

CHAPITRE 8

L'année à venir

À l'aube de 2011, nous nous attendons à une autre année remplie de défis à relever et de nouveaux enjeux.

Lorsque son mandat a été reconduit pour trois autres années en décembre 2010, la commissaire a déclaré qu'elle avait l'intention d'axer le reste de son mandat sur le leadership dans le cadre des enjeux prioritaires en matière de protection de la vie privée, l'appui aux Canadiennes et aux Canadiens, aux organisations et aux institutions pour qu'ils puissent prendre des décisions éclairées en matière de protection de la vie privée, et la prestation de services aux Canadiennes et aux Canadiens.

LEADERSHIP VIS-À-VIS DES ENJEUX PRIORITAIRES

Compte tenu que les Canadiennes et les Canadiens passent de plus en plus de temps dans l'environnement numérique, il est clair que c'est *là* que nous devons porter une grande partie de notre attention tout en continuant à nous acquitter de notre mandat qui est de faire respecter la LPRPDE. Ces enjeux sont cruciaux compte tenu du rôle que joue Internet dans la vie quotidienne des gens. Un grand nombre de Canadiennes et de Canadiens communiquent, magasinent, apprennent et pour ainsi dire *vivent* en ligne.

Nous continuerons d'améliorer notre connaissance des enjeux liés à la protection de la vie privée dans un monde numérique. Nous développerons notre expertise en informatique et créerons des liens avec des spécialistes externes.

Nous continuerons également de collaborer avec nos collègues territoriaux, provinciaux et étrangers.

SOUTENIR LA PRISE DE DÉCISIONS ÉCLAIRÉES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Pour protéger la vie privée, il faut aussi de veiller à ce que les Canadiennes et les Canadiens développent de solides compétences en matière de culture numérique. Nous continuerons d'employer des instruments en ligne et d'autres moyens novateurs pour aider les Canadiennes et les Canadiens à mieux comprendre leurs droits en matière de vie privée et à faire des choix éclairés dans un environnement qui évolue rapidement.

PRESTATION DE SERVICES

Nous continuerons de prendre des mesures pour garantir que nos activités répondent aux besoins et aux attentes des Canadiennes et des Canadiens. Nous tiendrons également compte des besoins des entreprises, du gouvernement et du Parlement.

Voici un aperçu de ce qui nous attend en 2011 :

DEMANDES DE RENSEIGNEMENTS ET ENQUÊTES

Nos fonctions d'enquête et de demande de renseignements constituent le service le plus direct offert par le Commissariat aux Canadiennes et aux Canadiens. Elles doivent donc bénéficier de la meilleure structure possible. Tandis que nous rédigeons ce rapport, nous mettons en œuvre certains changements dans notre structure organisationnelle, dont la création de deux unités d'enquête distinctes pour les plaintes qui relèvent de la *Loi sur la protection des renseignements personnels* et celles qui relèvent de la LPRPDE. Chaque unité aura son propre registraire des plaintes et sera responsable de ses propres fonctions de règlement rapide. La responsabilité de l'unité des demandes de renseignements sera confiée à la Direction des communications. Les fonctions d'enquête et de demande de renseignements, les services qui rejoignent le plus directement les Canadiennes et les Canadiens, disposera, grâce à cette nouvelle approche, ainsi de la meilleure structure de soutien possible.

LOI ANTIPOURRIEL

Compte tenu de l'adoption, à la fin de 2010, d'une loi visant à lutter contre les pourriels, nous nous préparons à collaborer avec les autres organismes chargés de l'application de cette loi, à savoir le Conseil de la radiodiffusion et des télécommunications canadiennes et le Bureau de la concurrence.

DISPOSITIONS LÉGISLATIVES TOUCHANT LA PROTECTION DE LA VIE PRIVÉE

Le deuxième examen parlementaire de la LPRPDE est prévu pour 2011.

Nous envisageons la possibilité de proposer des modifications qui permettraient de nous assurer que la loi reste un moyen efficace de protéger la vie privée des Canadiennes et des Canadiens. Par exemple, nous examinerons les conclusions d'une étude que nous avons commandée à deux universitaires de renom, qui ont été chargés d'analyser l'efficacité du modèle de l'ombudsman.

Nous attendons également avec impatience l'adoption éventuelle de modifications à la LPRPDE en vertu desquelles les organisations seraient tenues de signaler au Commissariat et aux personnes touchées les cas d'atteinte à la sécurité des renseignements personnels. Cette mesure législative était au stade de l'examen devant le Parlement à la fin de 2010.

CONSULTATIONS

Nous publierons le compte rendu final de nos consultations auprès des Canadiennes et des Canadiens au sujet du suivi, du profilage et du ciblage en ligne des consommateurs par les entreprises et de l'infonuagique. S'ensuivra l'accroissement de nos activités de sensibilisation visant le milieu technique et les petites et moyennes entreprises en offrant à ces derniers de l'information et des documents d'orientation plus ciblés. Nous comptons également poursuivre nos activités de sensibilisation auprès des jeunes et fournir plus d'information sur la protection de la vie privée aux parents.

SUR LA SCÈNE INTERNATIONALE

Nous continuerons d'affirmer le leadership du Canada dans les discussions internationales sur la façon d'améliorer les mesures de protection de la vie privée à l'échelle mondiale. Il s'agira notamment de collaborer avec des organisations comme la Coopération économique Asie-Pacifique (APEC), l'Organisation de coopération et de développement économiques (OCDE), le réseau ibéroaméricain de protection des données, l'Association francophone des autorités de protection des données personnelles (AFAPDP) et la Conférence internationale des commissaires à la protection des données et de la vie privée.

Nous prévoyons utiliser nos nouveaux pouvoirs législatifs pour partager de l'information avec nos homologues étrangers dans le but de régler des problèmes communs liés aux multinationales.

Nous sommes heureux que l'un de nos employés participe désormais aux réunions de la Commission de contrôle des dossiers d'INTERPOL, présidée par notre collègue de l'Irlande, le commissaire Billy Hawkes. Ce sera une occasion unique pour le Commissariat de connaître les enjeux de l'application du droit international et cela nous permettra de faire notre part pour qu'INTERPOL respecte les principes de la protection de la vie privée.

ANNEXE 1
Définitions et processus d'enquête

DÉFINITIONS DES TYPES DE PLAINTES DÉPOSÉES EN VERTU DE LA LPRPDE

Les plaintes adressées au Commissariat sont réparties selon les principes et les dispositions de la LPRPDE qui auraient été enfreints :

- **Accès.** Une personne s'est vue refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements, soit en raison d'une dispense dont l'organisation s'est prévalue pour retenir les renseignements.
- **Collecte**. Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.
- **Consentement.** Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement explicite de la personne concernée ou elle a fourni des biens et des services à la condition que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels.
- **Conservation.** Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins qu'une organisation a déclarées au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.
- **Correction/Annotation.** L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.
- **Délais.** Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la *Loi*.
- **Exactitude.** Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont exacts, complets et à jour.

- **Frais.** Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.
- **Mesures de sécurité.** Une organisation n'a pas protégé les renseignements personnels qu'elle détient par des mesures de sécurité appropriées.
- **Possibilité de porter plainte.** Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la *Loi* ou elle a enfreint ses propres procédures et politiques.
- **Responsabilité.** Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou qu'elle garde ou elle a omis de désigner une personne responsable de surveiller l'application de la Loi.
- **Transparence.** Une organisation a omis de rendre facilement accessible aux personnes des renseignements précis sur ses pratiques et politiques en matière de gestion des renseignements personnels.
- **Utilisation et communication.** Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles pour lesquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la Loi.

DÉFINITIONS DES CONCLUSIONS ET DES DÉCISIONS RELATIVES AUX PLAINTES

Le Commissariat a élaboré des définitions de conclusions et de décisions afin d'expliquer les résultats des enquêtes effectuées conformément à la LPRPDE :

- **Non fondée.** L'enquête n'a pas permis de déceler les éléments de preuves qui suffisent à conclure qu'une organisation a enfreint la LPRPDE.
- **Fondée.** L'organisation a contrevenu à une disposition de la LPRPDE.
- **Résolue.** L'enquête a corroboré les allégations, mais avant la fin de l'enquête, l'organisation a pris des mesures correctives pour remédier à la situation, à la satisfaction du Commissariat, ou s'est engagée à prendre ces mesures.
- **Fondée et résolue.** La commissaire est d'avis, au terme de son enquête, que les allégations semblent fondées sur des preuves, mais fait une recommandation à l'organisation concernée avant de rendre ses conclusions, et l'organisation prend ou s'engage à prendre les mesures correctives recommandées.

- **Réglée en cours d'enquête.** Le Commissariat aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. Aucune conclusion n'est rendue.
- **Abandonnée.** Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, lesquels sont essentiels pour en arriver à une conclusion.
- **Hors juridiction.** L'enquête a démontré que la LPRPDE ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.
- **Réglée rapidement.** Situation dans laquelle l'affaire est réglée avant même qu'une enquête officielle ne soit entreprise. À titre d'exemple, si une personne dépose une plainte concernant un sujet qui a déjà fait l'objet d'une enquête par le Commissariat et qui a été jugé conforme à la LPRPDE, nous donnons les explications nécessaires à la personne plaignante. Cette conclusion s'applique également lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du Commissariat.
- **Aucun rapport produit aux termes du paragraphe 13(2).** La commissaire n'est pas tenu de dresser un rapport si certaines conditions sont remplies : a) le plaignant devrait d'abord épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; b) la plainte pourrait être avantageusement instruite, dans un premier temps ou à toutes les étapes, selon des procédures prévues par le droit fédéral ou le droit provincial; c) le délai écoulé entre la date où l'objet de la plainte a pris naissance et celle du dépôt de celle-ci est tel que le rapport serait inutile; d) la plainte est futile, vexatoire ou entachée de mauvaise foi. S'il ne dresse pas de rapport, le commissaire informe le plaignant et l'organisation, en précisant les motifs.

PROCESSUS D'ENQUÊTE EN VERTU DE LA LPRPDE

Demande de renseignements

Une personne qui croit que la *Loi* a été enfreinte communique avec le CPVP par téléphone, par lettre ou en personne. Le personnel des demandes de renseignements fournit de l'information au sujet de la *Loi* et du rôle du Commissariat. Il est important pour nous de déterminer si la personne a tenté de régler l'affaire directement avec l'organisation. Dans plusieurs cas, on peut arriver à une solution rapidement et sans avoir recours à une enquête formelle.

↓

Plainte

Si le problème ne peut être résolu rapidement, le personnel des demandes de renseignements examine la question pour déterminer s'il s'agit bien d'une plainte, c'est-à-dire si les faits allégués représenteraient une infraction à la *Loi*.

Une personne peut déposer une plainte aux termes des articles 5 à 10 ou de l'annexe I de la *Loi* — par exemple, on lui aurait refusé l'accès à ses renseignements personnels ou de les lui fournir dans les délais prescrits par la *Loi*; on aurait recueilli, utilisé ou communiqué ses renseignements personnels de manière inappropriée; une organisation aurait utilisé ou communiqué des renseignements personnels inexacts au sujet de la personne ou ne disposerait pas de mesures de sécurité adéquate pour assurer la protection des renseignements personnels qu'elle détient.

Le personnel des demandes de renseignements aide la personne à formuler sa plainte. Notre formulaire de plainte en ligne fournit aux plaignants des renseignements détaillés sur l'information dont nous aurons besoin.

↓

Registraire des plaintes

Le registraire des plaintes examine chaque plainte pour s'assurer qu'il serait approprié que le Commissariat lance une enquête. Le registraire évalue également la complexité de la plainte et son degré de priorité, et détermine si elle pourrait être réglée rapidement.

Pas d'enquête

La personne est informée, par exemple, que la question ne correspond pas à notre champ de compétences.

Envoyée aux enquêtes

Une plainte de nature sérieuse, systémique ou autrement complexe — par exemple, questions de compétence incertaine, allégations multiples ou enjeux complexes sur le plan technique — est attribuée à un enquêteur.

Envoyée à un agent de résolution rapide

Une plainte qui, selon nous, pourrait être résolue rapidement est attribuée à un agent de résolution rapide. Sont incluses dans cette catégorie les plaintes sur des enjeux qui ont déjà fait l'objet de conclusions du Commissariat, celles où une organisation a déjà fait face aux allégations d'une manière que nous jugeons satisfaisante, et celles où il semble possible que les allégations pourraient être résolues facilement.

Enquête

Une enquête permet d'établir les faits; le commissaire détermine ensuite si le droit à la protection de la vie privée du plaignant en vertu de la LPRPDE a été enfreint.

L'enquêteur écrit à l'organisation pour lui présenter l'objet de la plainte. Il établit les faits grâce à l'audition d'arguments des deux parties, à la tenue d'une enquête indépendante, à l'interrogation des témoins et à l'examen de la documentation. L'enquêteur peut, de par les pouvoirs conférés par le commissaire ou par son délégué, recevoir des éléments de preuve, visiter les locaux de l'organisation au besoin et examiner ou se faire remettre des copies de documents trouvés dans les locaux visités.

Plainte abandonnée?

Il est possible qu'une plainte soit abandonnée dans des cas où, par exemple, la personne qui s'est plainte décide d'abandonner l'affaire ou est impossible à trouver.

Analyse (suite)

Plainte résolue? (suite)

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

Analyse

L'enquêteur analyse les faits et formule ses recommandations à l'intention du commissaire à la protection de la vie privée ou de son délégué. Il informe également les parties des recommandations fondées sur l'analyse des faits qu'il remettra au commissaire ou à son délégué. À cette étape, les parties peuvent faire d'autres auditions d'arguments.

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

Plainte résolue?

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

Conclusions

Le commissaire à la protection de la vie privée ou son délégué examine le dossier et évalue le rapport. Le commissaire ou son délégué, et non l'enquêteur, détermine les conclusions à tirer et décide s'il faut présenter des recommandations à l'organisation.

Rapport préliminaire

Si les résultats de l'enquête permettent de conclure qu'il y avait selon toute probabilité infraction à la LPRPDE, le commissaire à la protection de la vie privée ou son délégué recommande à l'organisation des mesures pour remédier au problème et lui demande de lui indiquer dans un délai précis comment elle entend mettre ces mesures en œuvre.

Rapport final et lettre de conclusions

Le commissaire ou son délégué envoie la lettre de conclusions d'enquêtes aux parties. Cette lettre présente la plainte, les faits établis, l'analyse et la réponse de l'organisation à toute recommandation faite dans le cadre du rapport préliminaire.

Les conclusions possibles sont les suivantes :

Non fondée : La preuve ne permet pas au commissaire à la protection de la vie privée ou à son délégué de conclure que le droit à la protection de la vie privée du plaignant en vertu de la LPRPDE a été enfreint.

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

Résolue : La preuve recueillie au cours de l'enquête donne raison au plaignant mais, avant que l'enquête ne soit terminée, l'organisation a pris ou s'est engagée à prendre des mesures pour corriger le problème.

Fondée et résolue : L'enquête donne raison au plaignant, et l'organisation a pris ou s'est engagée à prendre les mesures correctives recommandées dans le rapport préliminaire du commissaire, au terme de l'enquête.

Aucun rapport émis aux termes du paragraphe 13(2). Le commissaire n'est pas tenu de dresser un rapport si certaines conditions sont remplies : a) si le plaignant devrait d'abord épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; b) la plainte pourrait être avantageusement instruite, dans un premier temps ou à toutes les étapes, selon des procédures prévues par le droit fédéral ou le droit provincial; c) le délai écoulé entre la date où l'objet de la plainte a pris naissance et celle du dépôt de celle-ci est tel que le rapport serait inutile; ou d) la plainte est futile, vexatoire ou entachée de mauvaise foi. S'il ne dresse pas de rapport, le commissaire informe le plaignant et l'organisation, en précisant les motifs.

Dans la lettre de conclusions, le commissaire à la protection de la vie privée ou son délégué informe le plaignant de son droit de recours devant la Cour fédérale.

Lorsque des recommandations sont présentées à une organisation, des employés du CPVP effectuent un suivi pour vérifier si elles ont bel et bien été appliquées.

Le plaignant ou le commissaire à la protection de la vie privée peut choisir de demander une audience devant la Cour fédérale. La Cour fédérale a le pouvoir d'ordonner à une organisation de corriger ses pratiques ainsi que de publier un avis énonçant les mesures prises ou envisagées pour corriger ses pratiques. La Cour peut accorder des dommages et intérêts au plaignant, notamment en réparation de l'humiliation subie. Il n'existe pas de plafond pour ces dommages-intérêts.

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

ANNEXE 2

Statistiques sur les enquêtes liées à la LPRPDE pour 2010

Nota : Les pourcentages ayant été arrondis, leur somme peut ne pas être égale à 100.

STATISTIQUES SUR LES CAS DE RÈGLEMENT RAPIDE

Plaintes envoyées pour règlement rapide par secteur d'activité

	Nombre	Pourcentage
Secteur financier	21	19,4
Télécommunications	16	14,8
Services	14	13,0
Assurance	13	12,0
Autres	12	11,1
Vente/Détail	11	10,2
Transport	9	8,3
Hébergement	4	3,7
Santé	4	3,7
Divertissement	2	1,9
Services professionnels	2	1,9
Total	**108**	

Cas de règlement rapide par type de plainte

	Nombre	Pourcentage
Utilisation et communication	34	31,5
Accès	28	25,9
Collecte	19	17,6
Consentement	10	9,3
Conservation	6	5,6
Mesures de sécurité	5	4,6
Exactitude	2	1,9
Transparence	2	1,9
Correction/Annotation	1	0,9
Hors juridiction	1	0,9
Total	**108**	

Cas de règlement rapide par secteur d'activité

	Nombre	Pourcentage
Secteur financier	24	30,0
Vente/Détail	11	13,8
Autres	10	12,5
Télécommunications	10	12,5
Transport	6	7,5
Assurance	5	6,2
Services	5	6,2
Hébergement	4	5,0
Divertissement	2	2,5
Santé	2	2,5
Internet	1	1,3
Total	**80**	

Cas de règlement rapide fermés par type de plainte

	Nombre	Pourcentage
Utilisation et communication	27	33,8
Accès	23	28,8
Consentement	10	12,5
Collecte	8	10,0
Mesures de sécurité	5	6,3
Transparence	2	2,5
Conservation	2	2,5
Responsabilité	1	1,3
Exactitude	1	1,3
Correction/Annotation	1	1,3
Total	**80**	

STATISTIQUES DES CAS DE RÈGLEMENT RAPIDE ET DES PLAINTES OFFICIELLES

Cas de règlement rapide et plaintes officielles reçus par type de plainte

	2010				2009	
Type	Cas de règlement rapide	Plaintes officielles	Total	Pourcentage	Total	Pourcentage
Utilisation et communication	34	22	**56**	27	**59**	26
Accès	28	22	**50**	24	**64**	28
Collecte	19	14	**33**	16	**33**	14
Consentement	10	20	**30**	14	**22**	10
Mesures de sécurité	5	8	**13**	6	**21**	9
Conservation	6	4	**10**	5	**3**	1
Exactitude	2	2	**4**	2	**9**	4
Transparence	2	1	**3**	1	**4**	2
Détermination des fins de la collecte	0	2	**2**	1	**0**	0
Autres	1	1	**2**	1	**13**	6
Non-respect des principes	0	2	**2**	1	**2**	Moins de 1
Fins acceptables	0	1	**1**	Moins de1	**0**	0
Correction/ Annotation	1	0	**1**	Moins de1	**1**	Moins de 1
TOTAL	**108**	**99***	**207**	**100**	**231**	**100**

*_Nota_ : Quatre dossiers de règlement rapide ont été transmis aux enquêtes et figurent donc dans la colonne des plaintes officielles pour éviter le comptage double.

En 2010, nous avons reçu un total de 207 plaintes dans les deux catégories – les plaintes officielles (99) et les cas de règlement rapide (62 résolus et 46 en suspens) – au cours de 2010. Cela représente une diminution de 10 % comparativement aux 231 plaintes reçues en 2009.

Tel qu'il a été mentionné dans la rubrique 4.2, un total de 112 plaintes reçues par le Commissariat en 2010 ont été envoyées pour règlement rapide. Auparavant, ces cas auraient été acheminés directement aux enquêtes.

Des 112 cas de règlement rapide traités en 2010, 62 ont été résolus de manière satisfaisante, quatre n'ont pas été résolus et transférés aux enquêtes et 46 étaient en cours de traitement à la fin de l'exercice.

Les trois principaux types de plaintes sont restés les mêmes d'une année à l'autre.

Cas de règlement rapide et plaintes officielles reçus par secteur d'activité

Secteur	2010				2009	
	Cas de règlement rapide	Plaintes officielles	Total	Pourcentage	Total	Pourcentage
Secteur financier	21	24	45	22	55	24
Services	14	21	35	17	9	4
Assurance	13	14	27	13	41	18
Internet*	0	19	19	9	--	--
Télécommunications	16	3	19	9	42	18
Vente/Détail **	11	7	18	9	25	11
Transport	9	4	13	6	15	6
Hébergement	4	2	6	3	7	3
Services professionnels	2	4	6	3	10	4
Santé	4	0	4	2	8	3
Divertissement	2	0	2	1	0	0
Autres	12	1	13	6	19	8
Total			**207**	**100**	**231**	**100**

* Compte tenu du nombre croissant de plaintes reçues associées au monde numérique, nous considérons désormais les plaintes liées à Internet comme une catégorie à part entière. Auparavant, les plaintes associées à Internet étaient compilées dans la catégorie des télécommunications.

En 2010, 19 plaintes individuelles, ou 9 % de toutes les plaintes que nous avons reçues, étaient liées à Internet, ce qui en fait le troisième secteur en importance en matière de plaintes. Nous avions reçu 13 plaintes portant sur Internet en 2009, soit plus de 5 % du nombre total de plaintes.

** Le nom de cette catégorie était Vente, mais cela incluait les organisations de vente au détail.

DÉFINITIONS DES SECTEURS D'ACTIVITÉ

- **Secteur financier :** banques, intermédiation financière (p. ex. société émettrice de cartes de crédit, financement des ventes, prêts à la consommation, courtiers hypothécaires, activités de traitement des transactions financières), investissement financier et activités connexes, planification et investissement financiers, autorités monétaires.
- **Services :** organisations municipales et professionnelles, services de soins personnels, services de réparation et de soutien, programmes de récompense, services administratifs et de soutien (comprend les agences de recouvrement et les agences d'évaluation de crédit), services éducatifs et aide sociale.
- **Internet :** traitement des données, hébergement Web et services connexes, fournisseurs de services Internet, réseaux sociaux et portails de recherche Web.
- **Assurance :** sociétés d'assurance (responsabilité, vie, maladie, dommages).
- **Vente/Détail :** concessionnaires d'automobiles, matériaux de construction et fournisseurs, marketing direct, commerce électronique, vente au détail (en magasin et en ligne).
- **Services professionnels :** comptabilité, préparation de déclarations de revenus tenue des comptes et services de la paie, services juridiques, autres services professionnels, scientifiques et techniques.
- **Transport** : aérien, ferroviaire, transport en commun et transport terrestre de voyageurs, camionnage, transport par voie d'eau.
- **Télécommunications :** applications mobiles, entreprises de télécommunications par satellite, équipement de télécommunications, entreprises de télécommunications câblées ou sans fil.
- **Autres :** industries manufacturières, hors juridiction, diffuseurs (excepté Internet), alimentation et boissons.

Cas de règlement rapide et plaintes officielles par type de décision

	2010		2009	
Décision	**Cas**	**Pourcentage**	**Cas**	**Pourcentage**
Fondés et résolus	76	23	61	10
Règlement rapide	80	24	76	13
Non fondés	68	21	142	24
Résolus	32	10	51	9
Fondés	30	9	45	8
Abandonnés	18	6	118	20
Aucun rapport produit en vertu du par. 13(2)	9	3	4	1
Réglés	8	2	55	9
Hors juridiction	8	2	35	6
Total	**329 ***	**100**	**587**	**100**

* Comprend les 80 cas de règlement rapide et les 249 plaintes officielles.

Cas de règlement rapide et dossiers de plaintes fermés par type de plainte

	Fondés et résolus	Règlement rapide	Non fondés	Résolus	Fondés	Abandonnés	Aucun rapport en vertu du paragr. 13(2) 13(2)	Réglés	Hors juridiction	**Total**	**Pourcentage**
Accès	25	23	15	12	8	4	8	3	2	100	30
Utilisation et communication	22	27	18	6	12	4	1	1	1	92	28
Collecte	10	8	10	4	7	2	0	1	2	44	13
Consentement	8	10	10	2	1	1	0	0	2	34	10
Mesures de sécurité	6	5	7	2	1	3	0	2	1	27	8
Responsabilité	3	1	3	3	0	2	0	0	0	12	4
Exactitude	0	1	3	2	0	0	0	0	0	6	2
Conservation	1	2	0	0	0	1	0	1	0	5	2
Délais	1	0	1	0	1	1	0	0	0	4	1
Transparence	0	2	0	1	0	0	0	0	0	3	1
Correction/ Annotation	0	1	1	0	0	0	0	0	0	2	Moins de 1
Total	76	80	68	32	30	18	9	8	8	**329**	

Cas de règlement rapide et plaintes officielles par secteur d'activité

	Abandonnés	Hors juridiction	Non fondés	Aucun rapport produit en vertu du paragr. 13(2)	Résolus	Règlement rapide	Réglés	Fondés	Fondés et résolus	**Total**
Secteur financier	2	0	13	1	7	24	2	3	17	**69**
Assurance	0	3	23	7	12	5	2	5	6	**63**
Autres	0	0	5	0	3	10	2	11	10	**41**
Télécommunications	6	0	7	0	3	10	1	0	10	**37**
Services	0	3	3	0	4	5	0	3	13	**31**
Transport	1	0	3	0	2	6	0	4	4	**20**
Santé	1	0	8	0	1	2	0	2	5	**19**
Vente/Détail	3	0	2	0	0	11	0	2	1	**19**
Services professionnels	0	0	4	1	0	0	1	0	7	**13**
Internet	4	1	0	0	0	1	0	0	3	**9**
Hébergement	1	1	0	0	0	4	0	0	0	**6**
Divertissement	0	0	0	0	0	2	0	0	0	**2**
Total	18	8	68	9	32	80	8	30	76	**329**

« Services » comprend les services, les services administratifs et de soutien (inclut les agences de recouvrement et les agences d'évaluation de crédit) et l'aide sociale.

« Autres » comprend : les industries manufacturières, hors juridiction, les diffuseurs (excepté Internet), alimentation et boissons.

DÉLAIS DE TRAITEMENT

Délais de traitement moyens par types de plainte et de règlement

Type de plainte	Cas de règlement rapide		Plaintes officielles	
	Nombre	Délai de traitement moyen (mois)	Nombre	Délai de traitement moyen (mois)
Conservation	2	1	3	7
Correction/ Annotation	1	7	1	10
Mesures de sécurité	5	2	22	13
Transparence	2	4	1	15
Consentement	10	3	24	17
Exactitude	1	5	5	18
Accès	23	4	77	19
Responsabilité	1	2	11	18
Utilisation et communication	27	3	65	20
Délais	0	--	4	26
Collecte	8	2	36	26
	Total 80	**Moyenne pondérée 3,16**	**Total 249**	**Moyenne pondérée 19,4**

Délais de traitement moyens par type de décision

Décision	Nombre	Délai de traitement moyen (mois)
Règlement rapide	80	3
Réglé	8	6
Abandonné	18	11
Hors juridiction	8	14
Aucun rapport produit en vertu du paragr. 13(2)	9	16
Non fondé	68	18
Fondé et résolu	76	21
Résolu	32	22
Fondé	30	29
Total	**329**	**Moyenne pondérée 15,6**

Le délai de traitement est la période s'échelonnant de la date de *réception* de la plainte à la date à laquelle une conclusion est formulée ou une décision est prise relativement à cette plainte.

Dans les prochains rapports annuels, nous utiliserons une définition révisée du délai de traitement, qui sera désormais la période s'échelonnant de la date à laquelle la plainte est *acceptée* et la date à laquelle une conclusion est formulée ou une décision est prise relativement à cette plainte. Nous avons décidé de faire ce changement parce que la définition actuelle menait à des délais de traitement artificiellement longs. Dans plusieurs cas, par exemple, les plaintes que nous recevons ne contiennent pas toute l'information nécessaire pour commencer l'enquête. Nous ne pouvons amorcer notre travail si le dossier n'est pas complet.

Nous sommes heureux de constater que notre délai de traitement des plaintes est de 15,6 mois en 2010, comparativement à 18,5 mois l'année précédente.

La commissaire a déclaré que l'une de ses priorités au cours des trois prochaines années allait être l'amélioration de la prestation de services aux Canadiennes et aux Canadiens. À cette fin, nous continuerons à faire diminuer les délais de traitement des plaintes.

Avis volontaires d'incident lié à la sécurité des renseignements personnels – par secteur d'activité et type d'incident

	Communication accidentelle	Perte	Usurpation	Accès, utilisation ou communication non autorisés	Total
Hébergement	0	1	0	0	**1**
Services administratifs et de soutien	0	0	1	0	**1**
Construction	0	0	0	1	**1**
Divertissement	0	0	0	2	**2**
Services financiers	6	3	11	9	**29**
Santé	0	1	0	0	**1**
Assurance	1	0	0	1	**2**
Internet	1	0	0	0	**1**
Services professionnels	0	0	1	0	**1**
Vente/Détail	0	0	0	1	**1**
Services	0	1	0	0	**1**
Télécommunications	1	0	1	0	**2**
Transport	0	0	0	1	**1**
Total	**9**	**6**	**14**	**15**	**44**

Tel qu'il a été mentionné à la rubrique 4.8, nous souhaitons l'adoption de modifications législatives qui établiraient un système de signalement obligatoire.

En 2010, les deux tiers des signalements volontaires provenaient des institutions financières, lesquelles ont adopté des politiques de signalement proactif de ce type d'incident au Commissariat.

Dans plus du tiers des signalements d'atteinte, l'accès non autorisé à des renseignements personnels, souvent faits par les employés de l'organisation, était en cause. Presque autant d'incidents étaient associés au vol de renseignements personnels, notamment les vols d'ordinateurs portables.