Rapport annuel au Parlement 2014

PROTÉGER LA VIE PRIVÉE :

Une question d'intérêt mondial

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

Commissariat à la protection de la vie privée du Canada

Comme les flux d'information dans le monde moderne ne connaissent pas de frontières, les efforts de protection des données doivent eux aussi être internationaux.

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

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

© Ministre des Travaux publics et des Services gouvernementaux du Canada 2015

Nº de catalogue IP51-1F-PDF
1913-3375

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

Suivez-nous sur Twitter : @PriveePrivacy.

Commissaire à la protection de la vie privée du Canada

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

Privacy Commissioner of Canada

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

Juin 2015

L'honorable Leo Housakos, sénateur
Président
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2014.

Je vous prie d'agréer, Monsieur le Président, l'assurance de ma considération distinguée.

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

Original signé par

Daniel Therrien

Commissaire à la protection de la vie privée du Canada

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

Privacy Commissioner of Canada

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

Juin 2015

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

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2014.

Je vous prie d'agréer, Monsieur le Président, l'assurance de ma considération distinguée.

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

Original signé par

Daniel Therrien

Table des matières

À propos de la LPRPDE

La *Loi sur la protection des renseignements personnels et les documents électroniques*, ou 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 juste équilibre entre le droit à la protection des renseignements personnels des individus 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 recueillent, utilisent ou communiquent des renseignements personnels dans le cadre d'activités commerciales à l'échelle du pays, sauf dans les provinces disposant d'une loi essentiellement similaire sur la protection des renseignements personnels applicable au secteur privé. Le Québec, l'Alberta et la Colombie-Britannique disposent d'une telle loi. En outre, l'Ontario, le Nouveau-Brunswick et Terre-Neuve-et-Labrador ont promulgué des lois essentiellement similaires qui s'appliquent à certaines organisations du secteur de la santé.

Dans toutes les provinces, la LPRPDE s'applique aux activités du secteur privé sous réglementation fédérale. Elle protège également les renseignements sur les employés, mais uniquement dans le secteur privé sous réglementation fédérale.

Message du commissaire

Depuis que je suis commissaire à la protection de la vie privée, je suis frappé par le fait qu'un grand nombre de risques liés à la protection de la vie privée des Canadiens sont de nature mondiale.

En cette ère numérique, notre économie et notre société s'internationalisent de plus en plus, ce qui se traduit par un nombre croissant de renseignements personnels qui traversent les frontières. Un seul enjeu peut affecter un grand nombre de personnes dans plusieurs pays – comme nous l'avons constaté dans le cadre de nos enquêtes en 2014.

Dans un cas, par exemple, nous avons reçu plus d'une vingtaine de plaintes de Canadiens au sujet d'un site Web basé en Roumanie qui republie des jugements. Le site a ainsi rendu accessibles à toute personne ayant une connexion Internet de nombreuses décisions de tribunaux contenant des renseignements de nature très sensible relativement à des divorces, des gardes d'enfants, des faillites, des relations de travail, l'immigration, etc.

Une autre enquête a porté sur une importante atteinte à la sécurité des données chez Adobe Inc. qui a permis à des pirates informatiques d'accéder aux renseignements personnels de millions de clients partout dans le monde.

Pour les autorités responsables de la protection des données, comme le Commissariat à la protection de la vie privée du Canada, ces types d'enjeux rappellent l'importance de demeurer bien au fait des nouvelles tendances et de continuer à chercher des façons de collaborer plus étroitement avec leurs homologues provinciaux et internationaux.

Il devient essentiel de penser et de travailler à l'échelle mondiale, et c'est pourquoi les questions relatives à la protection de la vie privée de portée internationale occupent

une place centrale dans le Rapport annuel au Parlement de 2014.

Ce rapport met également en lumière l'augmentation remarquable du nombre de plaintes faites au Commissariat – le signe, peut-être, d'une préoccupation croissante du public à l'égard des questions de protection des renseignements personnels – et il décrit certaines des grandes enquêtes que nous avons faites au cours de l'année.

Ce rapport porte également sur la rapidité à laquelle les technologies (comme celles qui sont liées aux mégadonnées et à l'Internet des objets) évoluent et soulèvent de nouvelles préoccupations à l'égard de la protection de la vie privée. Il traite aussi des enjeux relatifs à la transparence qui sont associés aux demandes par le gouvernement à un accès à des renseignements personnels détenus par des entreprises du secteur privé, comme des fournisseurs de services de télécommunications.

COLLABORATION AVEC DES PARTENAIRES INTERNATIONAUX

Tous les jours, à chaque instant et partout dans le monde, on se fie à des technologies, à des plateformes et à des réseaux communs d'information et de communication. Les données touchées par ces activités en ligne peuvent voyager à l'échelle planétaire, notamment vers des entreprises tierces qui ne sont pas nécessairement assujetties à un régime de protection de la vie privée. Si une entreprise change ses pratiques en matière de protection des renseignements personnels, ou si elle est victime d'une atteinte à la sécurité des données, cela peut affecter des millions de personnes partout dans le monde.

C'est pourquoi, au cours des dernières années, le Commissariat a fait de la coopération internationale une priorité établie. Notre article de fond (voir la page 31) porte sur l'évolution de la collaboration internationale et sur certaines des mesures concrètes que nous avons prises avec nos partenaires internationaux en 2014. Il s'agit notamment du ratissage pour la protection de la vie privée du Global Privacy Enforcement Network, dans le cadre duquel 26 organismes d'application des lois sur la protection de la vie privée, coordonnés par le Commissariat, ont examiné comment des centaines d'applications mobiles populaires communiquaient leurs politiques sur la protection de la vie privée aux utilisateurs. Les préoccupations ainsi soulevées ont fait l'objet de mesures d'amélioration dans plus de 100 applications.

Les Canadiens tirent déjà profit des ententes de coopération que le Commissariat a établies avec ses homologues dans des pays comme l'Irlande et le Royaume-Uni, de même que les économies membres du Forum de coopération économique Asie-Pacifique. En 2014, nous avons ajouté Dubaï et la Roumanie à la liste des pays avec lesquels nous avons de telles ententes, ce qui nous permet de mener des enquêtes conjointes et, en conséquence, d'accroître notre efficacité à répondre aux préoccupations des consommateurs dans une économie mondiale de plus en plus dominée par les multinationales.

Parmi les moments forts de 2014, on note l'acceptation de l'Entente mondiale de coopération transfrontière dans l'application des lois par 55 autorités d'application des lois sur la protection des données dans le monde. Cette entente a pour but de favoriser la mise en place d'actions plus coordonnées pour traiter des questions de protection transfrontière des renseignements personnels. Elle répond à un besoin urgent qu'ont les autorités responsables de la protection des données de pouvoir partager de l'information confidentielle, ce qui permet une collaboration accrue et un plus grand nombre d'enquêtes conjointes.

C'est une avancée très positive. Lorsque l'Entente sera pleinement mise en œuvre, les organisations pourront faire des enquêtes ayant des répercussions mondiales dans le cadre d'un processus coordonné au lieu que chacune déploie les mêmes efforts que les autres dans le cadre d'une série d'enquêtes nationales. Dans de nombreux cas, les conclusions et résultats des enquêtes pourraient être publiés plus rapidement – renforçant et précisant ainsi les messages aux organisations et au grand public.

Il est dorénavant possible de dire que lorsqu'un incident ayant des répercussions internationales survient, les autorités responsables de la protection des renseignements personnels chercheront à déterminer avec quels partenaires il est le plus efficace de travailler, et de quelle manière.

Pour résumer, il s'agit d'une nouvelle façon de travailler.

Cette plus vaste collaboration devrait nous permettre d'assurer le respect des droits en matière de protection de la vie privée à une plus grande échelle qu'avant. Elle fournira également plus de recours aux personnes qui pourraient être préoccupées du fait qu'elles n'ont pas de contrôle sur leurs renseignements personnels dans un monde numérique sans frontières.

IMPORTANCE ACCRUE DES QUESTIONS ENTOURANT LES RENSEIGNEMENTS PERSONNELS

Au Canada et partout dans le monde, la question de la vie privée n'a jamais été aussi importante, et ce, de plusieurs façons. Les atteintes à la sécurité des données touchant de grands détaillants suscitent une vaste attention médiatique. Les interactions accrues entre les organisations responsables de l'application des lois, les organisations responsables de la sécurité nationale et les organisations commerciales qui détiennent des données sur les consommateurs ont soulevé la curiosité du public. De plus, la capacité accrue de suivre et d'analyser les comportements des consommateurs – en ligne et sur des appareils mobiles – amène les gens à se demander par qui, au juste, leurs renseignements personnels sont recueillis, où ils sont acheminés, comment ils sont utilisés et comment on peut avoir un plus grand contrôle sur eux.

Cet intérêt accru chez les consommateurs s'est entre autres traduit par une augmentation significative des requêtes et des plaintes au Commissariat en vertu de la LPRPDE en 2014.

RÉPONDRE AUX PRÉOCCUPATIONS ET GÉRER UNE DEMANDE ACCRUE

Bien que les plaintes en vertu de la LPRPDE aient augmenté de 50 % de 2013 à 2014[1], je suis heureux de souligner que l'efficacité des services offerts aux plaignants s'est accrue. Depuis 2012, le temps moyen affecté à une enquête relative à une nouvelle plainte a diminué de 3,5 mois.

Ce bon résultat découle du fait que le Commissariat a adopté une approche calibrée pour gérer les plaintes et cibler ses ressources en choisissant l'outil approprié pour régler des questions ayant trait à la protection de la vie privée. Par exemple, nous continuons de chercher des occasions d'utiliser notre processus efficace de règlement rapide des plaintes, ce qui nous permet de prendre en compte les préoccupations sans avoir à lancer une enquête officielle. Nous avons également exercé notre pouvoir de refuser d'entreprendre une enquête ou d'interrompre une enquête[2] lorsque nous l'avons jugé pertinent afin de concentrer nos ressources sur des questions qui soulèvent de plus grandes préoccupations ou qui ont de plus grandes répercussions.

SUIVRE LE RYTHME DES DÉVELOPPEMENTS TECHNOLOGIQUES

Notre niveau d'activité croissant et notre mission qui consiste à protéger et à promouvoir le droit à la vie privée nous obligent à cibler et à anticiper les questions émergentes concernant la protection de la vie privée. Au centre de plusieurs de ces questions se trouvent le rythme rapide et la portée sans cesse accrue du développement technologique.

Comme la connectivité des réseaux s'étend des ordinateurs et des dispositifs mobiles aux objets de tous les jours comme les voitures, les appareils électroménagers, les vêtements et les accessoires, la quantité de renseignements personnels qui est recueillie et distribuée augmente de façon importante. Lorsqu'elles sont exploitées et analysées, les données personnelles que ces appareils connectés peuvent recueillir en révèlent beaucoup au sujet de notre vie privée, notamment notre emplacement, nos habitudes de consommation et de déplacement, notre état de santé et même nos humeurs.

L'ère de l'Internet des objets et des accessoires intelligents ne fait que commencer, mais le Commissariat travaille déjà à s'assurer qu'il réagit efficacement à cette nouvelle réalité, notamment dans le cadre d'un programme de recherche visant à examiner les pratiques commerciales associées aux données qui ont recours à ces nouvelles technologies et à d'autres avancées techniques.

1 En 2014, nous avons accepté 402 plaintes en vertu de la LPRPDE. Si l'on soustrait les 170 plaintes concernant le Programme de publicité pertinente de Bell soumises en 2013 qui ont été traitées comme une seule plainte, les nouvelles plaintes ont augmenté de 55 % en 2014 par rapport à 2013.

2 En vertu du paragraphe 12.2 (1) de la LPRPDE, le commissaire « peut mettre fin à l'examen de la plainte s'il estime, selon le cas : *a*) qu'il n'existe pas suffisamment d'éléments de preuve pour le poursuivre; *b*) que la plainte est futile, vexatoire ou entachée de mauvaise foi; *c*) que l'organisation a apporté une réponse juste et équitable à la plainte; *d*) que la plainte fait déjà l'objet d'une enquête au titre de la présente partie; *e*) qu'il a déjà dressé un rapport sur l'objet de la plainte ».

En d'autres mots, nous devons continuellement améliorer notre compréhension des incidences pour la protection de la vie privée; déterminer quelles sont les meilleures façons de promouvoir et de garantir le respect de la confidentialité par les organisations du secteur privé; et promouvoir l'avantage concurrentiel que constitue la confiance accordée par les citoyens et les consommateurs. Nous avons hâte de partager de plus amples renseignements à ce sujet au cours de 2015.

TÉLÉCOMMUNICATIONS ET TRANSPARENCE

La protection de la vie privée est souvent synonyme de tendances nouvelles et émergentes, mais la question de l'accès par le gouvernement à l'information que détient le secteur privé, notamment aux données de télécommunications, continue de faire l'objet d'un important débat. Bien que nous comprenions qu'il est nécessaire d'avoir des mesures de sécurité et de renseignement adéquates, le Commissariat continue d'encourager les deux parties à faire preuve d'une plus grande transparence pour les Canadiens.

La décision de la Cour suprême du Canada dans *R.* c. *Spencer* a été à ce chapitre une étape importante. Dans cette décision unanime, la Cour suprême a maintenu qu'il existait une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonné à des services de télécommunications qui peuvent être révélés par l'étude de l'utilisation d'Internet, et qu'en l'absence de situation d'urgence ou d'une loi raisonnable, les responsables de l'application des lois devaient obtenir une autorisation préalable avant d'avoir accès à de telles données.

Toutefois, la question de savoir dans quelles circonstances une organisation serait autorisée à divulguer volontairement d'autres types de renseignements à la suite d'une demande de la police ou du gouvernement demeure sans réponse. Par conséquent, en novembre 2014, j'ai demandé au Parlement de fournir une orientation aux organisations et aux Canadiens afin que ces derniers comprennent mieux comment leurs renseignements personnels peuvent être divulgués aux pouvoirs publics sans leur consentement ou sans autorisation judiciaire.

Dans la foulée de l'arrêt *Spencer* de la Cour suprême et compte tenu des préoccupations des Canadiens au sujet de demandes d'accès non justifiées, nous accueillons favorablement la publication de rapports sur la transparence des entreprises et applaudissons les entreprises qui modifient leurs politiques à la lumière de cette décision. Nous travaillons également avec les fournisseurs de services et nous les encourageons à communiquer ouvertement combien de fois et dans quelles circonstances ils répondent aux demandes des autorités en vue d'obtenir des renseignements personnels.

Une telle transparence est essentielle à la protection de la vie privée. Elle informe les personnes de la façon dont leurs renseignements personnels seront utilisés, appuie leurs prises de décisions et crée pour les entreprises des occasions d'obtenir et de conserver la confiance des consommateurs.

APPUI À CERTAINS CHANGEMENTS PROPOSÉS À LA LPRPDE

La LPRPDE a été adoptée il y a plus de 10 ans dans le but d'accroître la confiance à l'égard de l'économie numérique. Les atteintes à la sécurité des données nuisent à la confiance des Canadiens. Par conséquent, nous accueillons favorablement la modification à la LPRPDE qui est demandée dans le projet de loi S-4, *Loi sur la protection des renseignements personnels numérique*, et qui vise à imposer la déclaration obligatoire des atteintes à la sécurité des données. En obligeant les organisations à nous informer de telles atteintes, nous serons en retour en mesure de travailler avec les entreprises pour les aider à répondre de façon adéquate et à mettre en place des pratiques qui empêcheront les incidents à l'avenir. La déclaration obligatoire donnera également une meilleure idée du type d'atteintes à la sécurité que subissent les organisations, ainsi que de la fréquence de telles atteintes.

La déclaration obligatoire permettrait de mieux informer les Canadiens des situations dans lesquelles leurs renseignements personnels ont été compromis. Elle permettait également au Canada de faire comme les autres gouvernements qui ont adopté des mesures similaires ou songent à le faire.

De plus, exiger des organisations qu'elles tiennent à jour un dossier des atteintes à la sécurité des renseignements et nous fournissent de l'information à cet égard serait un important mécanisme de reddition de comptes. Le Commissariat serait en mesure d'évaluer la conformité aux dispositions sur la notification de même que la façon dont les organisations décident ou non d'émettre des avis.

Nous attendons également avec impatience la mise en place d'ententes volontaires sur la conformité en vertu de la LPRPDE. Il s'agit là d'un outil qu'a demandé le Commissariat pour veiller à ce qu'une fois une enquête terminée, l'entreprise honore ses engagements à améliorer ses pratiques en matière de protection de la vie privée.

Bien que nous ayons des préoccupations concernant certaines autres dispositions du projet de loi (voir la page 29), les ententes volontaires sur la conformité et la déclaration obligatoire des atteintes sont des étapes positives dans la protection de la vie privée au Canada. En attendant, nous avons pris des mesures pour étendre notre capacité à répondre à de telles atteintes (voir la page 18).

PROCHAINES ÉTAPES

Pour ce qui est de l'avenir, j'estime que l'un des principaux défis de mon mandat est de veiller à ce que le Commissariat continue d'évoluer avec les nouvelles réalités en matière de protection de la vie privée.

Plus tôt dans mon mandat, j'ai annoncé vouloir engager un dialogue avec les intervenants de partout au pays en vue de nous aider à cerner quelles seraient nos priorités en matière de respect de la vie privée pour les cinq prochaines années. Ces priorités nous aideront à concentrer nos efforts et à guider les décisions concernant l'affectation de ressources

discrétionnaires dans le but d'accroître nos chances d'avoir une incidence bien réelle.

Au moment de la rédaction du présent rapport, le Commissariat a rencontré des intervenants des entreprises, du gouvernement, de groupes de défense des consommateurs, de la société civile et des universités afin de connaître leurs points de vue sur les domaines stratégiques qui menacent le plus la protection de la vie privée des Canadiens, et les domaines dans lesquels le Commissariat pourrait avoir le plus grand impact positif. Nous avons également mené des groupes de discussion avec des membres du grand public pour mieux comprendre leurs préoccupations et priorités en matière de protection de la vie privée.

Nous avons entendu de nombreux points de vue et nous établissons à présent les nouvelles priorités en matière de protection de la vie privée, que nous avons hâte de présenter au Parlement. Compte tenu du fait que les questions de confidentialité sont de plus en plus complexes et occupent une place grandissante, nous croyons que ces priorités nous aideront à préciser comment utiliser les ressources le mieux possible et améliorer notre capacité à protéger et à promouvoir les droits des Canadiens en matière de protection de la vie privée.

MOT DE LA FIN

Enfin, je m'en voudrais de ne pas mentionner le décès en 2014 de deux de mes prédécesseurs,

Bruce Phillips et George Radwanski. Ils ont occupé l'un après l'autre le rôle de commissaire, de 1991 à 2003.

Lorsqu'il était commissaire, M. Phillips a demandé au gouvernement fédéral d'adopter une loi sur la protection des renseignements personnels qui s'appliquerait au secteur privé. Ses efforts ont mené à l'adoption de la LPRPDE.

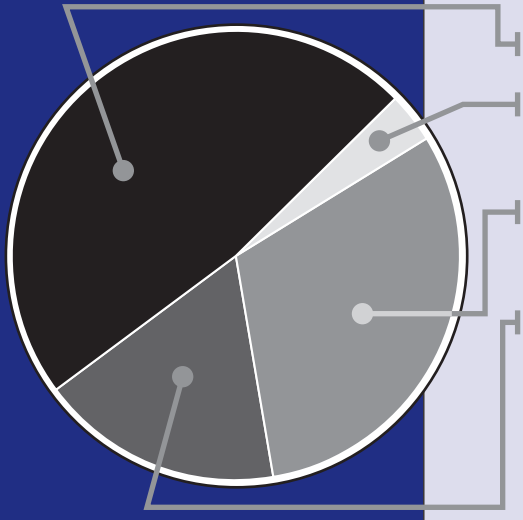
M. Radwanski était commissaire à l'entrée en vigueur de la LPRPDE et ses premières conclusions ont jeté les bases de la mise en œuvre de la *Loi*.

Lorsque je songe aux réalisations du Commissariat et que j'examine les nouveaux défis à relever, je peux dire avec confiance que nous sommes bien placés pour continuer à jouer efficacement notre rôle dans un monde en constante évolution.

La protection de la vie privée en chiffres en 2014

Plaintes acceptées	402

Nombre total des plaintes fermées (LPRPDE) : 375

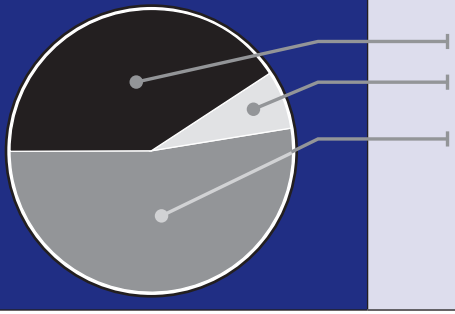


Plaintes fermées à l'issue d'un règlement rapide	**180**
Examens de plaintes auxquels on a mis fin en vertu de l'article 12.2[3] de la LPRPDE	**13**
Plaintes refusées, retirées ou hors du champ d'application du Commissariat	**117**
Plaintes fermées avec publication d'un rapport de conclusions	**65**
Plaintes jugées non fondées	25
Plaintes jugées fondées et résolues	24
Plaintes jugées fondées et conditionnellement résolues	7
Plaintes jugées fondées	2
Plaintes réglées en cours d'enquête	7

3 En vertu du paragraphe 12.2 (1) de la LPRPDE, le commissaire peut mettre fin à l'examen d'une plainte s'il estime, selon le cas : *a*) qu'il n'existe pas suffisamment d'éléments de preuve pour le poursuivre; *b*) que la plainte est futile, vexatoire ou entachée de mauvaise foi; *c*) que l'organisation a apporté une réponse juste et équitable à la plainte; *d*) que la plainte fait déjà l'objet d'une enquête au titre de la présente partie; *e*) qu'il a déjà dressé un rapport sur l'objet de la plainte.

Conformité par une application informelle	56

Nombre total de signalements d'atteinte à la LPRPDE : 44



Communication accidentelle	18
Perte	3
Vol et accès non autorisé	23

Demandes de renseignements en vertu de la LPRPDE	3 651
Consultations du site Web	3 370 692
Consultations du blogue du Commissariat	1 033 200
Consultations du canal YouTube du Commissariat	15 371
Gazouillis envoyés	437
Abonnés de Twitter au 31 décembre 2014	8 868
Documents d'orientation externes diffusés (secteur privé)	7
Ententes de contribution signées	14
Projets de loi et lois examinés quant à leurs répercussions sur la protection de la vie privée (secteur privé)	4
Comparutions devant des comités parlementaires (questions liées à la LPRPDE)	6
Mémoires officiels présentés (questions liées à la LPRPDE)	3
Échanges avec des parlementaires (secteur privé)	14

L'année en rétrospective

Nos diverses activités en 2014 – enquêtes, sensibilisation des intervenants, préparation à de nouvelles responsabilités en vue de l'application de la loi canadienne anti-pourriel, prestation de conseils et de renseignements au Parlement – reflètent la diversité des outils à la disposition du Commissariat pour protéger la vie privée et promouvoir les pratiques exemplaires au sein des organisations assujetties à la LPRPDE.

ENQUÊTES

Les Canadiens sont de plus en plus préoccupés par la façon dont les organisations du secteur privé traitent leurs renseignements personnels et ils s'adressent à nous pour obtenir de l'aide. L'équipe d'accueil a connu une autre année record en 2014, recevant un total de 1 238 demandes par écrit sur les questions de protection de la vie privée.

Nous avons aussi accepté 402 plaintes déposées en vertu de la LPRPDE, beaucoup plus que les quelque 250 nouveaux dossiers que nous ouvrons en moyenne par année. Comparativement à 2013 – et exception faite des 170 plaintes reçues cette année-là au sujet du Programme de publicité pertinente de Bell, qui ont fait l'objet d'une seule enquête entreprise par le commissaire –, les nouvelles plaintes ont augmenté de plus de 50 %.

En 2014, nous avons constaté une tendance selon laquelle de nombreuses plaintes sont déposées sur un même sujet. Par exemple, nous avons reçu :

- 27 plaintes contre le site Web Globe24h.com et sa façon de recueillir et de diffuser des renseignements personnels concernant des Canadiens (voir la page 34);

- 34 plaintes contre des entreprises de télécommunications découlant d'un projet universitaire sur les politiques de l'industrie en matière de conservation et de communication des données;

- 56 plaintes provenant de membres d'un syndicat sur un nouveau processus d'authentification mis en place par un transporteur aérien. (Dans ce cas, nous avons refusé d'enquêter, car une procédure de règlement des griefs par voie d'arbitrage était déjà en cours, ce qui pourrait régler la question.)

Compte tenu de l'intérêt accru des médias et du public au sujet des questions relatives à la protection de la vie privée, nous nous attendons à ce que cette tendance se maintienne. Néanmoins, malgré l'augmentation de la demande, nous sommes heureux de déclarer que les délais de traitement des plaintes continuent en fait de diminuer. Le délai de traitement moyen des nouvelles plaintes en 2014 était de 4,8 mois, par rapport à 5,3 mois en 2013 et à 8,3 mois en 2012.

Nous attribuons cette amélioration à notre approche calibrée de gestion des plaintes selon laquelle les ressources limitées servent à régler les questions qui préoccupent le plus la population canadienne. Ainsi, nous mettons l'accent sur le règlement rapide, les autres instruments de règlement et l'obtention de gains d'efficacité tout au long du processus d'enquête en utilisant l'outil adapté à la question particulière à traiter.

Les paragraphes suivants décrivent certaines enquêtes dignes de mention ainsi que les bons résultats que nous avons obtenus en utilisant nos divers outils de promotion de la conformité.

Manque de responsabilisation chez Microsoft

Un homme s'est plaint au Commissariat de ne pas avoir réussi à obtenir de la société Microsoft, même après des efforts considérables, qu'elle supprime son adresse de courriel de son compte client.

Notre enquête a révélé que l'incapacité de la société à répondre à la demande liée à la protection des renseignements personnels du client était principalement attribuable à un problème de conception technique, mais qu'elle était accentuée par d'importantes lacunes concernant la responsabilisation en matière de protection des renseignements personnels.

En raison d'un problème de conception technique non décelé auparavant, Microsoft ne pouvait pas supprimer l'adresse électronique du plaignant. Par conséquent, la société continuait de l'utiliser sans le consentement de celui-ci.

Fait plus troublant, cependant, aucun de la douzaine de représentants du service à la clientèle avec qui le plaignant a parlé de sa demande de suppression de son adresse de courriel – même ceux chargés précisément de régler les questions de protection de la vie privée – n'a reconnu que la préoccupation du plaignant était liée à la protection de la vie privée.

Bien que nous ayons pu constater pendant l'enquête que Microsoft avait consacré des ressources importantes à son programme de gestion de la protection de la vie privée et avait bien réfléchi à la question, il ressortait aussi clairement que ce programme comportait des lacunes se rapportant au soutien à la clientèle en matière de confidentialité. Par exemple, les représentants du service à la clientèle n'avaient pas reçu de formation suffisante pour reconnaître les problèmes de confidentialité et les transmettre au Centre de réponse pour la protection de la vie privée (Centre de réponse). En outre, les agents affectés à la protection de la vie privée n'avaient reçu aucune autre formation structurée sur la protection de la vie privée que celle suivie par les autres représentants du service à la clientèle.

Enfin, le personnel du Centre de réponse ne transmettait habituellement pas les problèmes de confidentialité non résolus au Bureau de protection de la vie privée de l'entreprise, qui, de son côté, ne surveillait pas les activités du Centre de réponse. Il y avait donc un problème de communication entre le Bureau de protection de la vie privée et le Centre de réponse, d'où la lacune en matière de responsabilisation à l'égard du traitement des préoccupations des clients relatives à la protection de leurs renseignements personnels.

Microsoft a répondu à la préoccupation initiale du plaignant et a résolu les problèmes de responsabilisation que nous avions décelés. La société a réglé le problème de conception du système sous-jacent, de manière à ce que les adresses de courriel puissent être supprimées dans les dossiers des comptes. Entre autres mesures, elle a aussi élaboré une formation spécialisée sur la protection de la vie privée à l'intention des représentants du service à la clientèle et a intensifié le niveau d'intervention du Bureau de protection de la vie privée dans la résolution des problèmes de confidentialité au moyen des diverses plateformes de soutien à la clientèle.

Une réponse insatisfaisante de Sobeys

Une femme a allégué qu'après avoir glissé dans une flaque d'eau à l'intérieur d'un supermarché en septembre 2011, elle est tombée et s'est blessée. À la suite de cet incident, elle a rempli le formulaire de rapport d'incident fourni par le supermarché.

À la fin de novembre 2011, elle a envoyé une lettre au siège social du supermarché dans laquelle elle décrivait certaines de ses préoccupations au sujet de l'incident et a demandé une copie du rapport d'incident, étant donné qu'on ne lui avait pas remis de copie sur le moment.

Bien que la plaignante soit parvenue à une entente de règlement avec l'entreprise au sujet de l'incident initial, elle a continué à lui demander par courriel d'avoir accès à ses renseignements personnels.

Le supermarché a répondu à la cliente à la fin d'août 2013, l'informant que sa plus récente demande avait été transmise aux « personnes appropriées ». Les noms de celles-ci n'étaient pas indiqués, et la plaignante n'a plus reçu de communications du supermarché, ni eu accès à ses renseignements personnels.

Pendant notre enquête, nous avons contacté Sobeys à plusieurs reprises. Toutefois, à notre grande déception, l'entreprise ne nous a pas répondu, n'a pas présenté d'observations ni participé au processus d'enquête. Nous avons conclu que Sobeys avait contrevenu à la LPRPDE en ne permettant pas à la femme d'avoir accès à ses renseignements personnels.

Après notre enquête, nous avons présenté à la Cour fédérale une demande d'audience sur la question. Sobeys a éventuellement fourni l'information que la femme recherchait, à notre satisfaction, et la procédure judiciaire a été abandonnée le 8 janvier 2015.

Protection de la vie privée des enfants

Une entreprise offrant des services destinés aux enfants et aux jeunes a la responsabilité particulière de veiller à ce que ces derniers et leurs parents puissent facilement prendre connaissance des services offerts, et comprendre les renseignements personnels qui sont recueillis, de quelles façons ils seront utilisés et à qui ils seront communiqués. Le Commissariat a ouvert une enquête sur les pratiques relatives à la protection de la vie privée du site canadien pour enfants populaire **www.webkinz.com** afin d'examiner certaines de ces importantes questions.

Notre enquête a permis de constater que, bien que le propriétaire du site Web, Ganz, se soit beaucoup soucié de la protection de la vie privée de ses jeunes utilisateurs (âgés de 6 à 13 ans) – qui s'inscrivent sur le site pour créer des animaux virtuels et en prendre soin, il y avait encore place à l'amélioration.

Lien

Conseils clés concernant la protection des renseignements personnels pour les services destinés aux enfants
https://www.priv.gc.ca/resource/fs-fi/02_05_d_62_tips_f.asp

Ressources concernant la vie privée des jeunes

La LPRPDE ne vise pas les enfants ou les jeunes en particulier, mais l'exigence pour les organisations d'obtenir un consentement valable fait en sorte qu'une attention particulière s'impose lorsqu'il s'agit d'enfants. En effet, le Commissariat a toujours considéré que les renseignements personnels des enfants et des jeunes étaient particulièrement sensibles. Les organisations qui recueillent, utilisent ou communiquent ces données doivent en tenir compte et se demander si ces renseignements personnels sont essentiels pour offrir des services appropriés en ligne.

Pour faire connaître les leçons tirées de l'enquête sur Ganz et deux autres dossiers antérieurs, nous avons diffusé une liste de conseils clés concernant la protection des renseignements personnels à l'intention des entreprises qui offrent des services destinés aux enfants et aux jeunes.

Elle s'ajoute à nos multiples ressources sur la protection de la vie privée élaborées pour les parents, les enseignants, les entreprises ainsi que les enfants et les jeunes euxmêmes.

Par exemple, l'entreprise n'utilisait pas un vocabulaire et des méthodes convenant à l'âge des utilisateurs pour dire clairement aux enfants de consulter leurs parents lors de leur inscription sur le site.

Ganz avait aussi accidentellement recueilli le nom complet d'enfants lorsque ceux-ci créaient leurs noms d'utilisateur. Nous craignions que ces renseignements, combinés à la collecte des adresses de courriel des parents et d'autres données, puissent permettre d'identifier les utilisateurs.

Des essais réalisés sur le site Web ont montré que certains annonceurs, à l'insu de Ganz, semblaient suivre l'activité des utilisateurs et qu'ils auraient donc pu établir le profil des enfants en fonction de leurs habitudes de navigation.

Ganz a pleinement collaboré à l'enquête et a accepté de mettre en œuvre un ensemble de mesures pour appliquer nos 11 recommandations dans un délai de neuf mois. Le Commissariat a donc jugé que les questions découlant de l'enquête sont fondées et conditionnellement résolues. Dans l'ensemble, nos constatations ont permis à Ganz et aux entreprises qui ont des sites Web destinés aux enfants de tirer des leçons, notamment celles-ci :

- Ne recueillez auprès des enfants que les renseignements personnels dont vous avez absolument besoin.

- Assurez-vous que les jeunes utilisateurs sont en mesure de comprendre l'information relative à la vie privée qu'ils fournissent, ou qu'ils comprennent bien qu'ils doivent consulter un adulte pour prendre une décision.

- Indiquez clairement *qui* doit accepter les conditions d'utilisation. On ne peut s'attendre à ce que des enfants « acceptent » des conditions rédigées en jargon juridique.

Le programme publicitaire de Bell soulève d'importantes préoccupations au sujet de la protection de la vie privée

En octobre 2013, le Commissariat a reçu un nombre sans précédent de plaintes à la suite du lancement du « Programme de publicité pertinente » de Bell. Ce programme prévoyait de suivre les activités des clients en ligne en matière de navigation sur Internet, d'utilisation des applications, d'appels téléphoniques et d'écoute de la télévision. Ensuite, en combinant ces renseignements avec les données démographiques des comptes recueillies dans les dossiers des clients, le programme créait des profils détaillés afin d'aider les annonceurs tiers à présenter des publicités ciblées aux abonnés de Bell, moyennant des frais.

Nous avons ouvert une enquête globale à la demande du commissaire pour examiner la portée complète des questions de protection de la vie privée soulevées dans les 170 plaintes reçues au sujet du programme.

Dans l'enquête, nous avons jugé que l'utilisation prévue des renseignements des clients par le programme était une « fin

acceptable » aux termes de la LPRPDE. Cependant, après avoir tenu compte du caractère sensible des renseignements utilisés et des attentes raisonnables de la part des clients concernant l'utilisation de leurs renseignements, nous avons conclu que Bell n'obtenait pas un consentement adéquat pour le programme. Bell imposait aux clients qui ne désiraient pas participer au programme d'avoir à prendre les mesures nécessaires pour s'en retirer, alors que nous avons conclu qu'il faudrait plutôt demander aux clients leur consentement à participer.

Bell, en tant que fournisseur de services de téléphonie, de sans-fil, d'Internet et de télévision, peut recueillir des données sur tous les sites que visitent ses clients, toutes les applications qu'ils utilisent, toutes les émissions de télévision qu'ils regardent et tous les appels téléphoniques qu'ils effectuent. Selon nous, la plupart de ces renseignements sont souvent de nature sensible et nous estimons que les renseignements servant à créer les profils peuvent probablement être considérés comme encore plus sensibles s'ils sont réunis pour dresser un portrait détaillé multidimensionnel de chaque abonné. De plus, le programme de Bell comportait une nouvelle utilisation des renseignements personnels des clients. Au départ, les clients fournissaient des renseignements personnels afin que l'entreprise puisse leur procurer des services de télécommunication et de distribution de radiodiffusion payants. Ce programme utilisait toutefois les renseignements personnels des clients dans le but secondaire de présenter des publicités comportementales ciblées de tiers. Nous étions d'avis que les clients de Bell s'attendaient raisonnablement à ce que l'entreprise obtienne leur consentement positif pour une telle pratique.

En 2011, le Commissariat a diffusé des lignes directrices sur la publicité comportementale en ligne. Celles-ci indiquent que le consentement negatif peut être approprié dans certaines circonstances. Lors de notre enquête sur Bell, toutefois, nous avons clairement établi que nos lignes directrices ne font pas du consentement négatif la forme de consentement à utiliser d'office. Lorsqu'elles déterminent la forme de consentement appropriée, les organisations devraient examiner soigneusement toutes les circonstances entourant leurs programmes de publicité comportementale ciblée, y compris les facteurs contextuels dont nous avons tenu compte dans l'enquête. Nos lignes directrices en matière de consentement en ligne, élaborées de concert avec nos homologues provinciaux en Alberta et en Colombie-Britannique et que nous avons présentées dans le rapport annuel 2013, énoncent des points clés que doivent examiner les organisations pour l'obtention d'un consentement valable en ligne.

Liens

Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne
https://www.priv.gc.ca/information/guide/2011/gl_ba_1112_f.asp

Lignes directrices en matière de consentement en ligne
https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_f.asp

De plus, notre enquête a permis de constater que Bell n'a pas respecté le choix des clients qui ont pris des mesures pour se retirer du programme. En effet, Bell a continué d'établir les profils de ces clients – dans l'éventualité où ils consentiraient un jour à participer au programme. Pour donner suite à notre recommandation, Bell a accepté, lorsqu'elle recevrait une demande de retrait, de cesser immédiatement de suivre les activités du client et de supprimer les renseignements de son profil individuel. L'entreprise a également accepté certaines recommandations, notamment :

- inclure des clauses dans ses contrats avec les annonceurs leur interdisant de lier les renseignements du profil provenant de Bell à une personne identifiable (c.-à-d. à partir de leurs propres fichiers-témoins, de l'empreinte de l'appareil électronique, des renseignements du compte ou d'autres méthodes de traçage);

- ne pas utiliser l'information relative à la cote de crédit dans ses profils de clients, une pratique que le Commissariat a jugée inappropriée;

- utiliser seulement des codes postaux partiels, plutôt que des codes complets, ce qui pourrait permettre de cibler un groupe beaucoup plus petit que prévu ;

- retirer La Source, un magasin de vente au détail de produits électroniques détenu par l'entreprise, de la liste des sociétés affiliées de Bell à qui celleci pourrait communiquer l'information recueillie.

À la suite de la conclusion de notre enquête, Bell a informé le Commissariat qu'elle avait décidé de retirer son programme et de supprimer tous les profils de clients existants liés à l'initiative. L'entreprise a depuis indiqué qu'elle prévoyait lancer un programme semblable dans l'avenir et qu'elle demanderait alors un consentement positif.

Bien que l'enquête soit maintenant considérée comme résolue, le Commissariat suivra de près les faits nouveaux dans cette affaire.

RÉCEPTION DES PLAINTES ET RÈGLEMENT RAPIDE

Notre unité de réception des plaintes joue un rôle important dans le choix de la meilleure façon de traiter les centaines de plaintes que nous recevons chaque année. La première étape consiste à examiner la plainte afin de voir si nous disposons de tous les renseignements requis pour l'accepter. Souvent, un agent de réception des plaintes encouragera les personnes à discuter du problème avec le chef de la protection des renseignements personnels de l'organisation, car il pourrait être en mesure de le régler immédiatement.

En 2014, nous avons fermé 180 dossiers de plainte grâce au processus de règlement rapide, soit une augmentation de 35 % par rapport à 2013. Nous continuons à favoriser cette approche utile et cherchons, chaque fois que cela convient, à faire participer les deux parties à un dialogue constructif dans le but de régler les questions de façon efficace et satisfaisante sans avoir à mener une enquête officielle qui demande beaucoup de temps et de ressources.

Nous sommes heureux d'indiquer que les organisations du secteur privé sont très souvent désireuses de répondre aux préoccupations relatives à la protection de la vie privée de leurs clients le plus rapidement possible. Les plaignants sont également heureux qu'on s'occupe de leurs demandes dans les meilleurs délais.

Exemples de règlement rapide

En 2014, par exemple, nous avons travaillé avec un commerce pour trouver une façon de recueillir des renseignements sur les clients qui louaient de l'équipement sans avoir à numériser leur permis de conduire. Le commerce a mis en œuvre la nouvelle politique et a formé son personnel en conséquence dans toutes ses succursales.

Dans un autre cas, nous avons réussi, sans ouvrir d'enquête officielle, à faire en sorte qu'un concessionnaire automobile supprime finalement les renseignements personnels d'un plaignant – notamment son numéro d'assurance sociale et une copie de son permis de conduire –, après qu'il l'ait demandé plusieurs fois sans succès.

ATTEINTES À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

En 2014, des entreprises ont volontairement déclaré 44 atteintes à la sécurité des renseignements personnels, comparativement à 60 en 2013. (Comme la déclaration des cas d'atteinte aux termes de la LPRPDE est facultative, nous ne sommes pas en mesure de dire s'il s'agit d'un changement dans le nombre réel d'atteintes ou d'une moins grande diligence en matière de signalement de la part des organisations.) En raison de l'importance des atteintes et des graves préjudices qui peuvent en résulter pour les personnes dont les renseignements sont compromis, nous avons assigné à un agent responsable de travailler avec les organisations qui ont subi une atteinte à la protection de leurs données. L'agent veille à ce que l'organisation mène à bien son enquête sur l'incident, avise les personnes touchées au besoin et mette en place des mesures pour empêcher que le problème ne se reproduise. Nous travaillons aussi régulièrement avec nos homologues provinciaux et internationaux sur des affaires d'atteinte à la protection des données, reconnaissant que celles-ci ont souvent des répercussions transfrontières considérables.

Plus du tiers (16) des atteintes signalées au Commissariat en 2014 provenaient d'organisations du secteur financier, et d'autres étaient issues du secteur Internet (7) et du secteur de l'assurance (6). Ces trois secteurs réunis ont totalisé près des deux tiers de toutes les atteintes.

Un émetteur de cartes de crédit prend immédiatement des mesures pour contrer une atteinte à la sécurité des données

Un émetteur de cartes de crédit a signalé au Commissariat qu'une erreur d'impression avait eu pour conséquence l'inclusion par mégarde des noms et des limites de crédit de certains titulaires de compte dans des lettres destinées à d'autres personnes. Dans l'ensemble, l'incident a touché 14 000 personnes.

Au cours de notre discussion avec l'entreprise, nous avons appris qu'elle menait une enquête sur la cause de l'atteinte, et qu'elle avait immédiatement informé toutes les personnes touchées par l'incident, désactivé leurs cartes de crédit et mis en place des contrôles additionnels pour la vérification des documents imprimés pour éviter que la situation ne se répète.

Plutôt que de juger les organisations uniquement en fonction d'incidents isolés, le Commissariat insiste sur l'importance pour elles de cerner et d'atténuer les risques afin de prévenir au départ de tels incidents, tout en étant préparées à agir promptement pour réduire les préjudices possibles en cas d'atteinte.

La majorité de ces incidents étaient attribuables soit au vol, soit à l'accès non autorisé à des renseignements personnels par des tiers non identifiés, des employés en place ou d'anciens employés. La deuxième cause la plus courante était la divulgation accidentelle de renseignements personnels par suite d'une erreur humaine ou d'un problème technologique.

Les mesures de protection insuffisantes et le stockage inutile rendent les données sensibles vulnérables

En octobre 2013, Peoples Trust, une institution financière sous réglementation fédérale qui a son siège à Vancouver, nous a signalé une atteinte à la sécurité des renseignements personnels. La confidentialité de renseignements personnels sensibles – dont le nom, la date de naissance, le numéro d'assurance sociale et le nom de jeune fille de la mère – de quelque 12 000 consommateurs avait été mise en péril après que ceux-ci les eurent fournis dans des applications en ligne pour faire un dépôt ou obtenir des produits de cartes de crédit avec garantie. L'incident ayant suscité plusieurs plaintes, nous avons ouvert une enquête à l'initiative du commissaire dans le but d'évaluer les mesures de protection de l'information et les pratiques de conservation de l'organisation.

L'enquête a révélé que, lorsqu'elle a conçu son portail Web des applications en ligne, l'entreprise n'a pas mis en place des mesures de protection suffisamment rigoureuses pour protéger les renseignements personnels sensibles recueillis auprès des consommateurs.

De plus, quand l'incident s'est produit, l'entreprise n'avait pas de politique exhaustive sur la sécurité de l'information.

Il y avait aussi des lacunes au chapitre de la surveillance et de la maintenance continues visant à repérer les vulnérabilités et les menaces numériques en constante évolution et à y remédier. Ainsi, sans que l'organisation le sache, une copie des renseignements des consommateurs – un double des données conservées dans la base de données interne de l'entreprise – a été stockée inutilement, sans être cryptée et à perpétuité sur un serveur Web qui n'avait pas été mis à jour pour faire face à une vulnérabilité bien connue. S'il n'y avait pas eu ce double inutile sur le serveur Web, la confidentialité de cette information n'aurait pas été mise en péril lors de l'incident.

Nous avons également constaté que Peoples Trust collaborait très bien avec le Commissariat durant l'enquête et que l'entreprise avait réagi à l'incident en temps opportun et de manière globale. Par exemple, elle a immédiatement embauché un consultant pour découvrir la cause de l'atteinte à la sécurité et « colmater la fuite ». Elle a aussi mis en place de nouvelles mesures pour aider les personnes touchées et réduire le risque d'incident à l'avenir.

Ces mesures consistaient entre autres à :

- envoyer des avis clairs et complets et à offrir des alertes de crédit aux personnes touchées par l'incident;
- mettre fin à la conservation inutile des renseignements personnels des consommateurs sur le serveur Web;
- améliorer les mesures technologiques pour protéger les renseignements recueillis en ligne;
- élaborer des procédures, et les messages internes connexes, pour renforcer les pratiques de protection de la vie privée, par exemple en exigeant une plus grande diligence dans le choix et l'embauche des tiers chargés de développer des systèmes de gestion de l'information.

Par conséquent, nous avons conclu que la plainte était fondée et qu'elle avait été résolue.

SENSIBILISATION DES INTERVENANTS

L'un des volets du mandat du Commissariat concerne la sensibilisation du public et, par conséquent, la tenue d'un dialogue avec les intervenants – les entreprises et les consommateurs – afin de les informer de la LPRPDE et de ses exigences; cela constitue une partie importante de nos activités. Les efforts de sensibilisation peuvent porter sur les nouveaux enjeux liés à la protection de la vie privée (particulièrement lorsque nous en apprenons plus sur les pratiques de l'industrie), les tendances et les défis, ainsi que les principales préoccupations des consommateurs. Grâce à nos efforts, nous établissons des relations avec les organisations assujetties à la *Loi* pour faciliter le règlement des plaintes. La sensibilisation et la formation sont des moyens

économiques d'accroître la conformité à la LPRPDE.

En 2014, nous avons réalisé de nombreuses activités de sensibilisation à la LPRPDE, notamment :

- une série de séances d'information à l'intention des intervenants partout au Canada en collaboration avec Industrie Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes avant l'entrée en vigueur de la loi canadienne anti-pourriel;

- une présentation devant le Conseil du district de l'Ontario de l'Organisme canadien de réglementation du commerce des valeurs mobilières, qui portait sur les facteurs relatifs à la protection de la vie privée dont les agents en placements doivent tenir compte pour se conformer aux exigences lorsqu'ils cherchent à obtenir des données sur la tolérance au risque, l'actif et le passif, et les sources de revenu du ménage en vue d'évaluer adéquatement la pertinence des transactions proposées aux clients;

- des allocutions lors d'événements axés sur la sécurité de l'information, par exemple : RSI 2014 (Rendez-vous de la sécurité de l'information), où nous avons examiné les défis que pose l'Internet des objets (pour en savoir plus sur le sujet, voir la page 24), et le Hackfest, où nous avons parlé principalement des atteintes à la vie privée et des métadonnées;

- participation à des conférences et à des foires importantes s'adressant aux industries dans lesquelles l'utilisation des renseignements personnels est en croissance, par exemple : DX3, une conférence annuelle pour les professionnels du marketing, de la publicité et de la vente au détail numériques; Restaurants Canada Show, qui s'adresse aux professionnels de la restauration et du tourisme d'accueil; et Fitness Business Canada, une conférence annuelle pour les professionnels du secteur du conditionnement physique;

- participation à des discussions dans de multiples forums concernant la prévention des atteintes à la sécurité des renseignements personnels et notre processus d'enquête lors de tels incidents.

En juin, nous avons publié des informations pratiques et utiles afin d'éclairer les organisations sur les mesures qu'elles peuvent prendre pour prévenir les incidents.

Dix conseils pour réduire le risque d'atteinte à la vie privée

Lien

Dix conseils pour réduire le risque d'atteinte à la vie privée
https://www.priv.gc.ca/resource/fs-fi/02_05_d_60_tips_f.asp

ENTRÉE EN VIGUEUR DE LA LOI ANTI-POURRIEL

Les principales dispositions de la loi canadienne anti-pourriel sont entrées en vigueur le 1er juillet 2014, y compris les modifications à la LPRPDE. Aux termes de la nouvelle loi, le mandat qui nous est confié concerne les deux domaines suivants :

- la collecte d'adresses électroniques, opération qui consiste à dresser des listes de courriels de masse au moyen de mécanismes parmi lesquels figure l'utilisation de programmes informatiques sondant automatiquement Internet en vue d'y trouver des adresses;

- la collecte de renseignements personnels par un accès illégal aux systèmes informatiques d'autrui, principalement à l'aide de logiciels espions.

Pour nous préparer à jouer notre rôle dans l'application conjointe de la nouvelle loi, nous avons conclu une entente de collaboration, de coordination et de communication de l'information avec nos partenaires, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence.

Ressources anti-pourriel

Nous avons mis à jour notre site Web en 2014 pour expliquer aux intervenants de l'industrie et au public nos responsabilités aux termes de la loi canadienne anti-pourriel. Au début de 2015, nous avons ajouté d'autres ressources utiles; voir la page : www.priv.gc.ca/lcap

Parmi les autres activités réalisées durant la première moitié de l'année, mentionnons :

- l'amélioration de nos processus d'enquête, de nos outils et du système de gestion des cas pour mieux nous adapter au fait que les enquêtes sont davantage fondées sur des renseignements que motivées par des plaintes, comme elles l'étaient traditionnellement;

- le renforcement des capacités d'analyse et de la sécurité de notre laboratoire technologique;

- la formation des enquêteurs et du personnel de première ligne du service de réception des plaintes et du Centre d'information.

Comme nous sommes l'un des partenaires de l'application de la loi canadienne anti-pourriel, nous avons accès aux observations faites par le public par l'entremise du site Web d'Industrie Canada (**www.combattrelepourriel.gc.ca**) et aux sources de données des tiers qui font rapport directement au Centre de notification des pourriels du CRTC. De concert avec notre analyste désigné du Centre (un poste financé par le Commissariat), nous avons passé la deuxième moitié de l'année 2014 à nous familiariser avec les fonctions du Centre et à analyser ses bases de données pour déceler les cas éventuels de collecte d'adresses et de logiciels espions qui pourraient faire l'objet d'une enquête. À la fin de l'année, nous avions lancé notre première enquête et nous étions en train d'évaluer d'autres cas potentiels.

POLITIQUES ET RECHERCHE

Notre fonction de recherche et d'élaboration de politiques appuie nos efforts de promotion et de protection du droit à la vie privée aux termes de la LPRPDE. Elle joue un rôle essentiel dans le développement de la position du Commissariat sur les nouveaux enjeux liés à la protection de la vie privée, et elle fournit une orientation aux organisations. Notre Programme des contributions favorise aussi le développement des connaissances et de l'expertise en matière de protection de la vie privée. Tous ces efforts contribuent à ce que nous soyons efficaces quand nous aidons les organisations à mieux protéger les renseignements personnels de la population canadienne au fur et à mesure que de nouveaux enjeux se profilent.

Conservation et retrait des renseignements personnels

À l'ère de l'information, un grand nombre d'organisations recueillent des renseignements personnels – sous forme physique ou électronique – dans le cadre de leurs activités quotidiennes. Ces renseignements sont obtenus auprès des citoyens, des employés, des clients et des clients potentiels. Comme le nombre d'organisations cherchant à tirer profit des mégadonnées augmente sans cesse, la pression n'a jamais été aussi forte pour amasser d'énormes quantités de renseignements personnels à des fins non encore déterminées. Cette capacité et ce désir toujours plus grands de recueillir, d'analyser et de conserver indéfiniment d'énormes quantités de renseignements personnels amplifient également les risques et les conséquences d'une atteinte éventuelle à la sécurité de ces renseignements. Les atteintes à la sécurité des renseignements personnels ne sont pas le seul sujet de préoccupation : plus l'information est conservée longtemps, plus le risque est grand qu'elle soit utilisée à des fins auxquelles les gens ne s'attendaient pas lorsqu'ils ont consenti à fournir leurs renseignements.

Une fois que des renseignements personnels ont été recueillis, les organisations doivent faire des choix éclairés quant à la durée de leur conservation, ainsi qu'au moment et à la façon de procéder à leur retrait.

En juin, nous avons publié des **lignes directrices** pour aider les organisations à adopter des politiques et des pratiques éclairées en matière de conservation et de retrait dans le cadre du traitement des renseignements personnels.

Ces lignes directrices portent sur les protocoles généraux en matière de collecte, de conservation et de retrait, et fournissent des renseignements pratiques pour le choix des méthodes de retrait et l'élaboration de politiques et de procédures fixant des calendriers de conservation et de retrait clairs.

Liens

Lignes directrices sur conservation et retrait
https://www.priv.gc.ca/information/pub/gd_rd_201406_f.asp

Document de recherche sur les accessoires intelligents
https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_f.asp

L'Internet des objets

Des recherches effectuées par le Commissariat en 2014 aideront les gens à comprendre comment leur vie privée peut être menacée par le réseautage en ligne d'une multitude d'objets du quotidien dotés d'une identification distincte – ce qu'il est convenu d'appeler l'Internet des objets.

Ces rapports de recherche traiteront de manière plus approfondie de certains des enjeux liés à la protection de la vie privée que le Commissariat a examinés dans le **document de recherche sur les accessoires intelligents**, publié en 2014.

Un document d'introduction présentera un aperçu des enjeux en question et établira le contexte pour les rapports complémentaires qui porteront quant à eux sur le suivi des décisions d'achat des consommateurs dans le commerce de détail et sur l'avènement des maisons et des appareils intelligents. Les rapports seront achevés et publiés plus tard en 2015.

Les mégadonnées et l'Internet des objets

Les mégadonnées et l'Internet des objets sont deux facettes importantes de l'explosion de la production, de la collecte et de l'utilisation des données à laquelle on assiste actuellement. Ces deux facettes ont des implications considérables pour la protection de la vie privée, et ce, tant au Canada qu'à l'étranger.

Comme le signalait le magazine *New Scientist*, grâce à un stockage moins coûteux, à un traitement plus rapide et à des algorithmes plus efficaces, les actions des gens peuvent être transformées en données. De leur côté, les organisations, par exemple les détaillants, peuvent effectuer une analyse et un forage de ces données pour en apprendre le plus possible sur le comportement antérieur des consommateurs dans le but d'affiner leurs stratégies commerciales et de développer de nouveaux produits et services.

Les capacités informatiques toujours plus grandes ont aussi débouché sur l'analyse des comportements futurs. L'« analyse prévisionnelle » peut procurer des avantages aux organisations commerciales. Elle peut contribuer à la création de nouveaux produits, à un marketing plus efficace et à des recherches mieux ciblées. Elle peut aussi entraîner des pratiques discriminatoires et invasives.

Avec l'avènement de l'Internet des objets, les mégadonnées ne pourront que prendre de l'ampleur. Cette évolution se profile déjà. En 2008, le nombre d'objets connectés à Internet dépassait déjà le nombre d'habitants sur la planète. Dans une étude Gartner publiée en décembre 2013, on estimait que 26 milliards d'appareils (sans compter les ordinateurs de bureau, les ordinateurs portatifs, les tablettes et les téléphones intelligents) seront connectés à Internet d'ici 2020.

Les capteurs intégrés à des objets interconnectés peuvent générer une quantité impressionnante de renseignements qu'il est possible de combiner, d'analyser et de mettre à profit, tout cela potentiellement sans la responsabilité, la transparence ou la sécurité appropriée, ou sans le consentement valable des intéressés. Le recoupement des renseignements recueillis peut servir à dresser un profil détaillé des personnes, ce qui suscite des préoccupations quant à la protection de la vie privée.

Dépistage génétique

Actuellement, il n'y a pas de loi au Canada qui porte expressément sur l'utilisation des résultats des tests génétiques par les compagnies d'assurance. Cela fait craindre que l'éventualité d'une discrimination génétique dissuade les gens de subir un test génétique, même quand ce serait souhaitable du point de vue clinique.

C'est pourquoi nous avons examiné les conséquences sur la vie privée qui découlent de la collecte et de l'utilisation des renseignements génétiques. Ce travail a donné lieu à la publication d'une **déclaration** concernant l'utilisation des résultats des tests génétiques par les compagnies d'assurances de personnes en juillet 2014.

Nous avons exhorté l'industrie à s'abstenir de demander les résultats des tests subis pour évaluer le risque à assurer jusqu'à ce que les assureurs puissent clairement démontrer que ces tests sont nécessaires et efficaces pour évaluer le risque.

Enfin, en octobre, le commissaire et deux représentants du Commissariat ont **comparu** devant le Comité sénatorial permanent des droits de la personne pour formuler des observations sur le projet de loi S-201. Ce projet de loi vise à empêcher les organisations d'exiger des personnes qu'elles subissent un test génétique ou qu'elles communiquent les résultats des tests subis pour obtenir des biens ou des services.

Déclaration du commissaire devant le Comité sénatorial permanent des droits de la personne, le 2 octobre 2014

« Le projet de loi S-201 reconnaît les avantages sociaux prépondérants d'une protection du droit à la vie privée des proposants et de l'offre d'une couverture d'assurance à tous, sans égard au patrimoine génétique. En outre, nous sommes encouragés par le fait que le gouvernement s'est engagé dans le discours du Trône à empêcher les employeurs et les compagnies d'assurance de faire de la discrimination sur la base d'analyses génétiques.

J'accueille favorablement le débat public que ce projet de loi génère, mais si la loi n'est pas adoptée, le Commissariat exhortera l'industrie de l'assurance, les groupes de défense des patients, les gouvernements fédéral et provinciaux et les autres parties intéressées à unir leurs efforts afin de trouver une solution non législative contraignante, comme celle existant au Royaume-Uni par exemple, pour s'assurer que les renseignements génétiques sont protégés de façon adéquate et utilisés uniquement lorsque cela est approprié et nécessaire. »

Liens

Déclaration concernant l'utilisation des résultats des tests génétiques
https://www.priv.gc.ca/media/nr-c/2014/s-d_140710_f.asp

Comparution concernant le projet de loi S-201
https://www.priv.gc.ca/parl/2014/parl_20141002_f.asp

Courtiers en données

Par « courtiers en données », on entend les entreprises qui recueillent des renseignements personnels sur les consommateurs auprès de diverses sources publiques et non publiques et les revendent à d'autres entreprises.[4]

Notre **document de recherche**, publié en septembre 2014, visait à fournir aux individus et aux entreprises une vue d'ensemble des exigences de conformité que doivent observer les courtiers en données dans le contexte de la protection de la vie privée au Canada et aux États-Unis.

Il est important de noter que le cadre exhaustif de conformité aux exigences de protection de la vie privée et à la réglementation dans lequel l'industrie du courtage de données au Canada exerce ses activités est différent du contexte observé aux États-Unis.

Dans une économie numérique intégrée et internationale, les données franchissent facilement les frontières et les organisations ont accès aux renseignements personnels grâce à des moyens nouveaux et innovateurs. Il est difficile de savoir si les courtiers en données de l'étranger connaissent la LPRPDE et se conforment à ses exigences lorsqu'ils font affaire au Canada.

Au fur et à mesure que les courtiers seront informés de ces exigences, ils comprendront mieux leurs obligations, et il leur sera plus facile de mettre au point des pratiques favorisant le contrôle par les consommateurs, la confiance et la transparence. De leur côté, les consommateurs qui auront de l'information sur les courtiers en données et sur leurs pratiques seront davantage en mesure de prendre des décisions éclairées concernant leurs renseignements personnels lorsqu'il s'agit de donner leur consentement et d'exercer un contrôle.

Lien

Document de recherche
https://www.priv.gc.ca/information/research-recherche/2014/db_201409_f.asp

4 Federal Trade Commission, « FTC to Study Data Broker Industry's Collection and Use of Consumer Data », communiqué, 18 décembre 2012 [anglais seulement].

Évaluation du Programme des contributions du Commissariat

Créé en 2004, le Programme des contributions du Commissariat à la protection de la vie privée finance la recherche indépendante et les initiatives connexes d'application des connaissances portant sur la protection de la vie privée. Au cours de l'exercice 2014-2015, le Programme a octroyé plus de 470 000 $ pour financer neuf nouveaux projets indépendants de recherche et d'application des connaissances. Ces projets vont permettre d'acquérir et de diffuser de nouvelles connaissances sur les risques en matière de vie privée et sur les mesures de protection que peuvent appliquer les institutions gouvernementales, les organisations et les citoyens canadiens. Voici quelques exemples des projets de l'an dernier :

- **étude de la technologie des véhicules intelligents;**
- **documentaire sur la protection de la vie privée et les données généalogiques;**
- **analyse des politiques de confidentialité des prêteurs sur salaire en ligne;**
- **étude de la protection des renseignements personnels concernant la santé mentale;**
- **application pour renseigner les jeunes sur la protection de la vie privée en ligne.**

Le Programme a également alloué des fonds pour l'organisation et l'accueil du troisième symposium de recherche Parcours de protection de la vie privée. Cette série de symposiums a été instaurée par le Commissariat en 2012 dans le but de faire connaître davantage les résultats des projets de recherche et d'application des connaissances dans le domaine de la protection de la vie privée au Canada. Le troisième symposium, qui a eu lieu en février 2015, s'est déroulé sous le thème « Retour aux principes premiers de la protection de la vie privée à l'heure des avancées technologiques ». Il a offert l'occasion d'examiner les valeurs à la base de la protection de la vie privée et de déterminer en quoi les avancées technologiques et scientifiques favorisent ou menacent ces valeurs.

Comme pour tous les programmes de contributions administrés par les institutions fédérales, une évaluation indépendante du rendement et de la pertinence doit être faite tous les cinq ans. La dernière évaluation a été effectuée en 2014, après quoi le Programme a été renouvelé pour une autre période de cinq ans.

ACTIVITÉS PARLEMENTAIRES

En juin 2014, le Commissariat a présenté un mémoire au Comité sénatorial permanent des transports et des communications, puis il a comparu devant le Comité pour parler des diverses modifications proposées à la LPRPDE dans le cadre du projet de loi S-4, *Loi sur la protection des renseignements personnels numériques*.

Dans notre mémoire et lors de notre comparution, nous avons accueilli favorablement les propositions visant à rendre obligatoire la déclaration des incidents liés à la protection des renseignements personnels et à renforcer les exigences en matière de consentement et les dispositions sur l'accord de conformité volontaire – des mesures grâce auxquelles nous pourrons plus facilement nous assurer que les entreprises respectent les engagements pris au terme des enquêtes. De façon générale, nous étions également en faveur des autres modifications proposées pour remédier aux problèmes et aux lacunes apparus depuis l'entrée en vigueur de la LPRPDE.

Nous avons cependant exprimé des réserves concernant deux des ajouts proposés – les alinéas 7(3)*d.1*) et 7(3)*d.2*) – qui, dans certaines circonstances, autoriseraient une organisation à communiquer des renseignements personnels à une autre organisation sans le consentement de l'intéressé. Nous avons fait valoir que ces deux nouveaux alinéas pourraient entraîner une communication excessive dont ni les personnes intéressées ni le Commissariat ne seraient au courant.

Autres activités parlementaires notables

- **Comparution devant le Comité sénatorial des transports et des communications au sujet de la pratique consistant à recueillir et à analyser les données des clients de Bell à des fins commerciales, notamment à des fins de publicité ciblée (29 avril 2014)**
- **Comparution devant le Comité sénatorial permanent des finances nationales concernant le projet de loi C-31, *Loi nº 1 sur le plan d'action économique de 2014* (13 mai 2014; mémoire)**
- **Comparution devant le Comité permanent de la justice et des droits de la personne (JUST) de la Chambre des communes concernant le projet de loi C-13, *Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle* (10 juin 2014; mémoire)**
- **Comparution devant le Comité sénatorial permanent des droits de la personne concernant le projet de loi S-201, *Loi visant à interdire et à prévenir la discrimination génétique, Loi sur la non-discrimination génétique* (2 octobre 2014)**

Liens

Comparution au sujet du Bell
https://www.priv.gc.ca/parl/2014/parl_20140429_cb_f.asp

Comparution concernant le projet de loi C-31
https://www.priv.gc.ca/parl/2014/parl_20140513_cb_f.asp

Mémoire présenté sur le projet de loi C-31
https://www.priv.gc.ca/parl/2014/parl_sub_140512_sen_f.asp

Comparution concernant le projet de loi C-13
https://www.priv.gc.ca/parl/2014/parl_20140610_f.asp

Mémoire présenté sur le projet de loi C-13
https://www.priv.gc.ca/parl/2014/parl_sub_140609_f.asp

Comparution concernant le projet de loi S-201
https://www.priv.gc.ca/parl/2014/parl_20141002_f.asp

De plus, nous recommandons qu'on exige des organisations « qu'elles rendent public le nombre de communications effectuées à des autorités chargées de l'application de la loi en vertu de l'alinéa 7(3)*c.1*), à l'insu de l'intéressé et sans son consentement, et sans mandat, afin de faire la lumière sur la fréquence à laquelle cette exception extraordinaire est invoquée et sur l'utilisation qui en est faite ».

Lien

Mémoire présenté sur le projet de loi S-4
https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_f.asp

On peut consulter la version intégrale de notre **mémoire** sur notre site Web.

Article de fond

Protéger la vie privée : Une question d'intérêt mondial

En 2014, la protection de la vie privée a beaucoup retenu l'attention – peut-être comme jamais auparavant. Ce fut aussi une année marquante pour la collaboration internationale entre les autorités chargées de l'application des lois sur la protection de la vie privée.

Au cours de l'année, les relations et les réseaux soigneusement cultivés depuis plus d'une décennie ont mené à des interventions pour la protection de la vie privée sur de nombreux fronts internationaux.

Plus que jamais, alors que les Canadiens bénéficient des avantages inégalés de l'ère numérique et de l'économie sans frontières qui en découle, le Commissariat intensifie sa collaboration avec ses homologues internationaux pour réduire autant que possible les risques connexes en matière d'atteinte à la vie privée.

Après des années d'expansion graduelle de nos activités, de nos relations et de nos réseaux internationaux, l'année 2014 a vu les mesures d'application internationales passer à une vitesse supérieure, et elle devient de ce fait le nouveau point de référence.

Les citoyens canadiens craignent que les mécanismes de protection de la vie privée soient plus faibles, et aussi d'avoir moins accès à des recours pour régler les problèmes lorsque leurs renseignements personnels traversent les frontières du pays.

Compte tenu de ces préoccupations, il est essentiel d'accroître sans cesse la collaboration internationale pour établir et maintenir la confiance dans l'économie numérique mondiale d'aujourd'hui.

Au cours de l'année, nous avons :

- formulé un nouvel accord international avec nos homologues, qui favorisera une collaboration encore plus grande entre les organismes d'application des lois sur la protection de la vie privée de partout dans le monde;
- coordonné un ratissage mondial qui visait à accroître la sensibilisation aux pratiques des applications mobiles en matière de protection de la vie privée et qui a débouché sur des initiatives favorisant la transparence de ces pratiques dans l'intérêt des utilisateurs des applications;
- mené une enquête au nom des citoyens canadiens dont les renseignements personnels liés à des procédures judiciaires ont été rendus entièrement accessibles, notamment par l'entremise des moteurs de recherche, par un site Web basé en Roumanie;
- participé à une intervention avec deux autres pays à la suite d'une atteinte à la sécurité des données d'envergure mondiale qui a touché des millions de personnes;
- participé aux efforts qui ont amené les opérateurs à décider de fermer un site Web basé en Europe de l'Est qui diffusait des images prises par des caméras Web non protégées, y compris des caméras qui se trouvaient dans les chambres à coucher de citoyens canadiens.

Liens

Autorités de protection de la vie privée de la zone Asie Pacifique [anglais seulement]
http://www.appaforum.org/about/

Association francophone des autorités de protection des données personelles
http://www.afapdp.org/

Commission de contrôle des fichiers d'INTERPOL
http://www.interpol.int/fr/Internet/À-propos-d'INTERPOL/Structure-et-gouvernance/CCF/La-Commission-de-contrôle-des-fichiers-d'INTERPOL

Groupe de travail international sur la protection des données dans les télécommunications (Groupe de Berlin) [anglais seulement]
http://www.berlin-group.org/

Autres initiatives internationales notables

- **Autorités de protection de la vie privée de la zone Asie Pacifique [anglais seulement] : Ce groupe se réunit deux fois par année pour échanger des idées et des pratiques exemplaires au sujet de la réglementation sur la protection de la vie privée, les nouvelles technologies et les moyens d'accroître la sensibilisation aux enjeux à ce chapitre.**
- **Association francophone des autorités de protection des données personnelles : Nous avons contribué à la création de cette organisation en 2007. Elle représente les autorités francophones de protection des données du monde entier et aide les pays en développement de la Francophonie à établir des régimes de protection des données.**
- **Commission de contrôle des fichiers d'INTERPOL : Le Commissariat participe aux réunions de cette instance, qui sert d'organisme indépendant afin de surveiller si INTERPOL respecte les normes établies pour le traitement des renseignements personnels.**
- **Groupe de travail international sur la protection des données dans les télécommunications (Groupe de Berlin) [anglais seulement] : Ce groupe examine les avancées technologiques qui soulèvent des enjeux de protection de la vie privée, et il se concentre sur les renseignements personnels sur Internet.**

ACCROÎTRE LA PARTICIPATION ET CONJUGUER NOS EFFORTS

Les fondements des interventions de l'an dernier ont été posés dans les 10 années précédentes. En 2004, nous avons considérablement intensifié notre participation aux initiatives internationales. Cette année-là, nous avons assisté à une première réunion du Groupe de Berlin (voir l'encadré). Au cours des deux années suivantes, nous avons participé pour la première fois aux réunions de l'Organisation de coopération et de développement économiques (OCDE) et de l'Organisation de coopération économique Asie-Pacifique (APEC).

En juin 2007, les pays membres de l'OCDE ont adopté la Recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée. Entre autres choses, la recommandation exhortait les pays membres à modifier leurs lois pour permettre aux autorités de collaborer, et elle préconisait la création d'un réseau informel des autorités chargées de l'application des lois sur la protection de la vie privée.

Par la suite, en mars 2010, nous nous sommes joints à 10 autres autorités pour établir le **Global Privacy Enforcement Network** (GPEN) [anglais seulement] afin de favoriser la coopération transfrontière entre nous.

La même année, l'**Accord de coopération de l'APEC sur la protection transfrontière des données** [anglais seulement] est entré en vigueur. Aux termes de cet accord, les pays membres ont convenu de collaborer aux enquêtes sur la protection de la vie privée des consommateurs et aux initiatives d'application de la loi.

CHANGEMENT IMPORTANT MENANT À DES INTERVENTIONS ET À DES RÉSULTATS

Environ quatre ans après la Recommandation de l'OCDE, les modifications apportées à la LPRPDE en 2011 nous ont permis de conclure des accords écrits officiels avec d'autres autorités chargées de l'application des lois sur la protection de la vie privée du Canada et de l'étranger. Ainsi, nous pouvons maintenant échanger de l'information avec d'autres organisations aux fins de l'application des lois tout en protégeant la confidentialité des renseignements.

Depuis, nous avons signé des protocoles d'entente avec nos homologues de l'Allemagne, de l'Irlande, des Pays-Bas, du Royaume-Uni et de l'Uruguay. En 2013, notre entente avec nos homologues néerlandais nous a permis de mener à terme la première **enquête mondiale conjointe**, qui portait sur le service de messagerie mobile multiplateforme de WhatsApp.

Les possibilités de collaboration de ce genre nous aident également à accroître notre capacité dans le domaine de l'application des lois relatives aux pourriels. Par exemple, nous avons intensifié notre participation au Plan d'action de Londres et au Groupe de travail de la messagerie, des maliciels et de la lutte contre l'abus à l'aide d'appareils mobiles, deux réseaux internationaux importants dans la sphère de

Liens

Global Privacy Enforcement Network (GPEN) [anglais seulement]
https://www.privacyenforcement.net/

l'Accord de coopération de l'APEC sur la protection transfrontière des données [anglais seulement]
http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

Enquête sur WhatsApp
https://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_f.asp

l'élimination des pourriels qui regroupent un nombre considérable de membres de l'industrie. Cet engagement nous permet de tirer profit de l'expérience des autorités qui veillent à l'application de lois anti-pourriel en vigueur depuis longtemps et d'entretenir des partenariats en vue d'une future coopération en matière d'application de la loi.

UNE ANNÉE CHARNIÈRE SUR LA SCÈNE INTERNATIONALE POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

En 2014, en plus de signer de nouvelles ententes de collaboration avec nos homologues à Dubaï et en Roumanie, nous avons pris part à plusieurs enquêtes et activités d'application des règles où nous avons pu échanger des renseignements et conjuger nos efforts.

Facturer la vie privée

En 2014, le Commissariat a reçu 27 plaintes concernant le site Web roumain Globe24h.com et sa façon de recueillir les renseignements personnels de Canadiens pour ensuite les publier. En raison des similitudes entre les plaintes, nous les avons traitées dans le cadre d'une même enquête.

Globe24h.com republie les conclusions juridiques provenant de différentes régions, dont un grand nombre du Canada. Avant l'ère numérique, l'inclusion des renseignements personnels dans les décisions écrites des tribunaux avait des répercussions très limitées. En bref, pour trouver des renseignements sensibles sur un particulier qui étaient contenus dans une décision, il fallait d'abord se présenter au tribunal ou aux archives pour ensuite devoir procéder à une recherche rigoureuse.

Aujourd'hui, bien entendu, l'information numérique est à portée de main. Contrairement à d'autres répertoires de décisions juridiques en ligne, Globe24h.com autorise les moteurs de recherche à indexer les pages, ce qui augmente de beaucoup l'accessibilité des renseignements personnels contenus dans les conclusions.

Dans tous les cas, Globe24h.com avait publié une décision de la cour qui contenait des renseignements personnels sensibles sur les plaignants.

Environ un tiers des plaintes déposées au Commissariat concernaient des affaires de droit de la famille, comme un divorce ou des audiences sur la garde d'enfants. Les autres plaintes portaient sur des causes de faillite, de droits de la personne, de relations de travail et d'immigration. Les documents publiés contenaient des renseignements personnels détaillés très sensibles, notamment des données sur la situation financière ou la santé qui pourraient avoir des effets adverses sur la réputation de la personne en cause.

Par exemple, une des plaintes a été faite au nom de la fille du plaignant, décrite comme une « travailleuse du sexe » dans une cause où elle a témoigné. Au moment du dépôt de la plainte, la décision, telle que publiée par Globe24h.com, était le premier document qui apparaissait lorsqu'on faisait une recherche en ligne du nom de la personne.

Dans une autre affaire, la plaignante était préoccupée par le fait qu'une recherche en ligne avec le nom de son fils menait à des renseignements sur une audience pour garde d'enfants houleuse.

Un homme a déposé une plainte car il exploitait une entreprise portant son nom et se disait préoccupé par le fait que les recherches sur cette entreprise menaient également à des renseignements sur sa situation financière et médicale qui avaient été dévoilés dans le cadre d'une poursuite.

Un autre homme considérait que la publication de conclusions juridiques annulerait la valeur du pardon qu'il a obtenu.

Profitant du caractère sensible des renseignements publiés et des nombreuses demandes déposées pour les faire retirer, l'entreprise a établi des processus formels et informels de demande de retrait d'information de son site Web, moyennant certains frais. Selon nous, cette pratique de la part de Globe24h.com revient à monnayer de l'information et à extorquer des paiements pour qu'elle soit retirée.

Par exemple, lors du dépôt de la première plainte au Commissariat, les particuliers pouvaient demander un retrait rapide de l'information, soit dans les 72 heures, moyennant des frais de traitement de 19 euros (environ 25 $) par document. En juillet 2014, alors que notre enquête était en cours, cette option payante a été supprimée du site Web. Malgré tout, une plaignante a rapporté que Globe24h.com l'avait informée que son dossier pouvait être retiré complètement des serveurs de l'entreprise et de Google pour la somme de 200 euros (environ 266 $).

Dans presque tous les cas, le Commissariat a pu faire retirer les documents offensants du site Web sans frais, même s'il subsiste des préoccupations quant au fonctionnement général du site.

Pour ces raisons, et étant donné l'emplacement du site Web, le Commissariat a conclu un accord de coopération avec l'autorité de la protection des données de la Roumanie, qui a également reçu des plaintes au sujet de l'entreprise, afin de trouver une solution appropriée. Le Commissariat poursuit ses activités en vue de donner suite à ses conclusions de plusieurs façons.

Protections insuffisantes contre une atteinte internationale

En 2013, les médias ont rapporté une intrusion complexe à long terme des systèmes informatiques de l'entreprise Adobe inc., intrusion qui touchait des millions de consommateurs dans le monde entier. Un particulier a déposé une plainte auprès du Commissariat après avoir retrouvé les renseignements personnels relatifs à son compte Adobe sur un site Web public, après qu'on lui ait dit que l'atteinte ne l'affectait pas.

Par la suite, une enquête conjointe entre le Commissariat et le commissaire à la protection des données de l'Irlande, menée en collaboration avec l'autorité de la protection des données de l'Australie, a permis de conclure

que les mesures de protection mises en place par Adobe au moment de l'intrusion étaient insuffisantes compte tenu du caractère sensible des données en cause (noms d'utilisateur, mots de passe, noms et adresses, numéros de carte de crédit cryptés). Nous sommes convaincus qu'Adobe a mené une enquête approfondie sur cette atteinte et apporté des changements afin de protéger les données des consommateurs, par exemple en améliorant son processus de gestion des mots de passe et en mettant hors service un serveur touché par l'atteinte.

Comme les effets de l'atteinte touchaient le monde entier, il nous appartenait de collaborer avec des partenaires internationaux pour protéger les renseignements personnels des particuliers au pays et à l'étranger.

Avertissement au sujet des caméras Web

En plus d'élargir la portée de tout organisme responsable de la protection des données, la collaboration et la coordination ajoutent la force du nombre aux activités d'application de la loi en plus de permettre une intervention plus rapide lorsque la situation l'exige. Par exemple, en 2014, nous avons rapidement pu mobiliser un grand nombre de nos homologues pour traiter une violation de la vie privée ayant cours dans le monde entier.

À la mi-novembre, le Commissariat s'est penché sur un site Web hébergé en Europe de l'Est qui affichait des liens vers des images tirées de caméras Web non sécurisées de partout sur la planète, y compris le Canada. Ce geste visait à démontrer les dangers de ne pas modifier le nom d'utilisateur et le mot de passe par défaut du fabricant. Le résultat net de cette initiative a été que des images de résidences, de lieux de travail et d'espaces commerciaux ont été rendues accessibles à tous, tout comme dans de nombreux cas l'emplacement exact de la caméra.

Lorsque nous avons été mis au courant de l'existence du site Web, nous avons rapidement communiqué avec d'autres autorités chargées de la protection des renseignements personnels, qui étaient également préoccupées par la situation. Le Commissariat, en collaboration avec les responsables des autorités de la protection des données du Royaume-Uni, de l'Australie et de Macao ainsi qu'avec les commissaires du Québec, de l'Alberta et de la Colombie-Britannique, a envoyé une lettre aux exploitants du site Web pour les presser de supprimer ces fils.

Nous avons été heureux de constater que les exploitants du site Web ont tenu compte de nos préoccupations et ont fermé le site après l'envoi de la lettre. Depuis ce temps, une version réduite du site Web a été remise en ligne, et propose essentiellement des liens vers des caméras Web présentes dans des endroits publics.

Forts de ces résultats, nous avons ensuite collaboré avec nos homologues pour rédiger des **lettres d'information** destinées aux fabricants de caméras Web les pressant de mettre en place des mesures de sécurité adéquates pour protéger la vie privée de leurs clients et de fournir plus de conseils aux clients sur les moyens de protéger leurs caméras Web.

Lien

Lettres d'information
https://www.priv.gc.ca/media/nr-c/2015/let_150212_f.asp

Un ratissage qui montre des pratiques douteuses

En tant que coordonnateur du deuxième **ratissage pour la protection de la vie privée du Global Privacy Enforcement Network (GPEN)**, le Commissariat s'est inspiré du succès du premier événement, tenu en 2013, en rassemblant des représentants d'organismes de la protection des données de partout au monde afin de s'attaquer à une question précise liée à la protection des renseignements personnels. Au total, 26 autorités chargées d'assurer la protection des renseignements personnels ont participé au ratissage de 2014, comparativement à 19 à celui de 2013.

Le thème de 2014 était les applications mobiles. En tout, les organismes participants ont évalué plus de 1 200 des applications mobiles les plus populaires au monde (le Commissariat en a évalué 151) pour voir les types d'autorisations qui étaient demandés, déterminer si ces demandes excédaient les attentes compte tenu des fonctions de l'application et, plus important encore, établir de quelle manière on expliquait aux utilisateurs les raisons pour lesquelles les renseignements étaient demandés et à quoi ils étaient censés servir.

Dans l'ensemble, bien que le **ratissage** ait permis de constater que de nombreuses applications populaires suscitent la confiance de l'utilisateur en fournissant rapidement des explications claires et faciles à lire sur les renseignements recueillis et leurs utilisations, de nombreuses autres applications ne donnent

Le Commissariat à la protection de la vie privée continue à jouer un rôle prédominant au sein d'un réseau international

En plus de coordonner le ratissage annuel pour la protection de la vie privée du GPEN, le Commissariat est aussi un des cinq pays membres du comité de gestion du GPEN, avec le Royaume-Uni, la Nouvelle-Zélande, Israël et les États-Unis. Le Commissariat offre un soutien technique pour le site Web du GPEN, lequel est hébergé par l'OCDE. Parmi les changements apportés en 2014, mentionnons l'ajout d'une liste de personnes-ressources pour l'application des lois à l'OCDE, à l'APEC et au Conseil de l'Europe ainsi que l'amélioration de la plateforme de communications publiques du GPEN.

De manière générale, en 2014, le GPEN a connu énormément de succès en appuyant la collaboration pour l'application internationale des lois sur la protection de la vie privée. De plus, le nombre d'autorités membres a augmenté de 50 % pour atteindre 51 membres, et la communication entre les autorités sur le site Web sécurisé augmente aussi.

Liens

Ratissage international pour la protection de la vie privée du GPEN
https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_f.asp

Résultats du ratissage
https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_f.asp

aucun renseignement de base sur la protection de la vie privée. Par exemple, 85 % des applications évaluées ne précisent pas comment les renseignements personnels des utilisateurs sont recueillis, utilisés ou communiqués.

À la suite du ratissage, nous avons regroupé les leçons apprises et rédigé des conseils pratiques pour les développeurs d'applications. Le document résultant s'intitule **Dix conseils pour faire connaître les pratiques en matière de protection de la vie privée aux utilisateurs de votre application**.

Pour donner suite aux préoccupations concernant certaines applications, nous avons envoyé des lettres, qui ont mené à l'amélioration des pratiques en matière de protection des renseignements personnels pour plus de 100 applications, tant au Canada qu'à l'étranger.

Préciser ce qui attend le consommateur dans les boutiques virtuelles d'applications

À la suite du ratissage, nous avons uni nos efforts à ceux du commissaire à la protection des données personnelles de Hong Kong pour encourager les boutiques virtuelles d'applications, comme celles exploitées par Apple et Google, à faire preuve d'une transparence accrue en exigeant des développeurs qu'ils affichent des liens vers leurs politiques sur la protection des renseignements personnels. En collaboration avec 23 de nos homologues sur la scène internationale, nous avons d'ailleurs **publié** une lettre ouverte à ce sujet au début décembre.

Liens

Dix conseils pour faire connaître les pratiques en matière de protection de la vie privée aux utilisateurs de votre application
https://www.priv.gc.ca/resource/fs-fi/02_05_d_61_tips_f.asp

Lettre ouverte
https://www.priv.gc.ca/media/nr-c/2014/let_141210_f.asp

L'Entente mondiale de coopération transfrontière dans l'application des lois n'est pas la seule initiative de collaboration annoncée à Maurice. Les agences responsables de la protection des données du Commonwealth y ont également convenu de créer le Common Thread Network. Ce groupe a pour objectif de faciliter l'échange d'expérience, de connaissances et d'expertise et de promouvoir la collaboration transfrontière entre les différents membres du Commonwealth. Les membres fondateurs ont également reconnu le rôle qu'une protection des données adéquates peut jouer dans la croissance des technologies de l'information et des communications, ce qui, en retour, stimule le développement socioéconomique.

Une nouvelle approche multilatérale élargie

Les ententes bilatérales et les initiatives régionales visant à promouvoir la collaboration ont sans aucun doute appuyé nos efforts d'application des lois sur la protection des renseignements personnels. Cependant, les différentes voies que prennent les renseignements en cette ère de la technologie exigent que l'échange d'information et les activités d'application des lois soient coordonnés à une échelle plus large du point de vue international afin que les autorités puissent en faire plus, plus rapidement.

Pour y parvenir, en 2014, les autorités de protection des renseignements personnels de partout dans le monde ont franchi une étape importante.

L'Entente mondiale de coopération transfrontière dans l'application des lois est le résultat de la collaboration et d'une planification commune des participants à la Conférence internationale des commissaires à la protection des données et de la vie privée. Annoncée à la Conférence de 2014, qui se tenait à Maurice, l'Entente établira des fondements communs favorisant un échange d'information rapide ainsi que la collaboration entre les autorités de la protection des renseignements personnels du monde entier pour ce qui est de l'application de la loi.

La nouvelle entente établit des règles de base sur l'échange de renseignements confidentiels dans le cadre des activités d'application de la loi. Par exemple, ces règles pourraient autoriser plusieurs autorités de la protection des données à collaborer pour réagir à une atteinte majeure à la sécurité des données. La capacité d'échanger ce type d'information est cruciale pour coordonner les activités d'application de la loi. Pour nous, ce mécanisme multilatéral est un ajout précieux aux ententes bilatérales et aux protocoles d'entente déjà en place.

Nous sommes fiers d'avoir co-dirigé avec nos homologues du Royaume-Uni la rédaction des documents qui détaillent cette nouvelle approche de l'application des lois sur la protection des renseignements personnels.

PROCHAINES ÉTAPES

L'Entente mondiale de coopération transfrontière dans l'application des lois, qui doit entrer en vigueur dès octobre 2015, pourrait bien être l'entente de protection des renseignements personnels la plus vaste au monde, offrant ainsi un moyen efficace aux organismes chargés de la protection des données de profiter du travail d'application des lois des autres et de renforcer les activités de protection des renseignements personnels en général.

De plus, en conjuguant nos efforts, nous pourrons envoyer un message plus clair et plus fort aux multinationales qui doivent respecter diverses lois sur la protection des renseignements personnels partout dans le monde, afin de les inciter à améliorer leurs pratiques en matière de protection de la vie privée.

Le soutien accordé à cette entente dans le monde entier par les commissaires à la protection des données et des renseignements personnels ainsi que la participation grandissante au GPEN (la planification du ratissage sur la vie privée de 2015 est déjà en cours) et à d'autres initiatives internationales mettent en évidence l'importance que la communauté de la protection de la vie privée accorde à la collaboration pour améliorer la protection des renseignements personnels.

De plus en plus, lorsqu'il est question de protection des renseignements personnels, la collaboration internationale est nécessairement de mise. Le Commissariat sait à quel point la collaboration internationale est essentielle et

peut affirmer avec confiance que les Canadiens profiteront des retombées de son travail, qui vise à protéger leurs renseignements personnels, peu importe le lieu où ils se trouvent.

Une collaboration accrue entre les organismes chargés de la protection des renseignements personnels peut renforcer la confiance des citoyens, habiliter les particuliers à participer à l'économie numérique mondiale sans crainte et les inciter à adopter de nouveaux produits et services avec confiance plutôt qu'appréhension.

Au bout du compte, ce résultat profitera à tous.

Statistiques relatives aux enquêtes

LPRPDE 2014 - **NOMBRE DE PLAINTES FERMÉES, PAR TYPE ET PAR DÉCISION**

Type de plainte	Réglée rapidement	Fin de l'examen (article 12.2)	Refusée	Hors du champ d'application	Retirée	Réglée	Non fondée	Fondée	Fondée et résolue	Fondée et conditionnellement résolue	Total
Accès	50	4			8	3	2	1	9		**77**
Utilisation et communication	35	5		7	14		6		6		**73**
Collecte	29	1		5	9	1	14	1		1	**61**
Fins appropriées	1	2	56							1	**60**
Mesures de sécurité	24	1			11	1	1		2		**40**
Consentement	16				5	2	2		1	3	**29**
Délais	11								1		**12**
Exactitude	5				2				2		**9**
Rétention	7								1		**8**
Responsabilité	2								1		**3**
Correction/annotation	0								1		**1**
Explication des fins	0									1	**1**
Transparence										1	**1**
Total	**180**	**13**	**56**	**12**	**49**	**7**	**25**	**2**	**24**	**7**	**375**

LPRPDE 2014 - **DÉLAI DE TRAITEMENT MOYEN, PAR DÉCISION**

Décision	Nombre	Délai de traitement moyen en mois
Réglée au processus de règelment rapide	180	2,4
Résolue	7	6,8
Fin de l'examen (article 12.2)	13	5,7
Retirée	49	6,0
Hors du champ d'application	12	7,8
Non fondée	25	12,4
Fondée et conditionnellement résolue	7	27,4
Fondée et résolue	24	11,5
Fondée	2	15,5
Refus d'enquêter	56	0,6
Nombre total de cas	**375**	
Moyenne générale pondérée		**4,8**

LPRPDE 2014 - **DÉLAI DE TRAITEMENT DES PLAINTES EN VERTU DE LA LPRPDE** – Délai de traitement moyen, par type de plainte et de règlement

	Réglée rapidement		Autres formes de règlements (pas de règlement rapide)	
Type de plainte	**Nombre de cas**	**Délai de traitement moyen en mois**	**Nombre de cas**	**Délai de traitement moyen en mois**
Accès	50	2,7	27	10,4
Responsabilité	2	7,4	1	15,8
Exactitude	5	3,0	4	8,9
Fins appropriées	1	3,4	59	1,0
Collecte	29	2,8	32	10,3
Consentement	16	2,3	13	13,5
Correction/annotation			1	10,6
Explication des fins			1	30,9
Transparence			1	30,9
Conservation	7	2,1	1	15,1
Mesures de sécurité	24	2,5	16	6,9
Délais	11	1,5	1	3,4
Utilisation et communication	35	1,8	38	6,9
Total	**180**	**2,4**	**195**	**7,0**

LPRPDE 2014 - **AVIS VOLONTAIRE DE MANQUEMENTS À LA LPRPDE,** par secteur de l'industrie et par type d'incident

Secteur	Type d'incident			Nombre total d'incidents par secteur	Proportion de tous les incidents
	Divulgation accidentelle	Perte	Vol et accès non autorisé		
Hébergement			1	1	2 %
Finances	9	2	5	16	36 %
Assurances	2		4	6	14 %
Internet	1		6	7	16 %
Autres secteurs	1			1	2 %
Professionnels			1	1	2 %
Vente/commerce de détail	2		3	5	11 %
Services	1	1	1	3	7 %
Télécommunications	1		2	3	7 %
Transports	1			1	2 %
Grand Total	**18**	**3**	**23**	**44**	**100 %**

LPRPDE 2014 - **PLAINTES ACCEPTÉES, PAR SECTEUR DE L'INDUSTRIE**

Secteur	Nombre	Proportion des plaintes acceptées
Hébergement	19	5 %
Divertissement	4	1 %
Finances	81	20 %
Assurances	21	5 %
Internet	72	18 %
Autres secteurs	24	6 %
Professionnels	9	2 %
Vente/commerce de détail	25	6 %
Services	23	6 %
Télécommunications	52	13 %
Transports	72	18 %
Total	**402**	**100 %**

LPRPDE 2014 - **PLAINTES ACCEPTÉES, PAR TYPE DE PLAINTE**

Type de plainte	Nombre	Proportion des plaintes acceptées
Accès	77	19 %
Responsabilité	3	0 %
Exactitude	8	2 %
Fins appropriées	60	15 %
Collecte	65	16 %
Consentement	47	11 %
Conservation	7	1 %
Mesures de sécurité	33	7 %
Délais	12	7 %
Utilisation et communication	90	22 %
Grand Total	**402**	**100 %**

LPRPDE 2014 - **PLAINTES FERMÉES, PAR SECTEUR DE L'INDUSTRIE ET PAR DÉCISION**

Secteur	Règlement rapide	Décision (pas de règlement rapide)									Total partiel des décisions (excluant les règlements rapides)	Total des règlements rapides et des autres décisions
		Refusée	Fin de l'examen (article 12.2)	Hors du champ d'application	Retirée	Réglée	Non fondée	Fondée	Fondée et résolue	Fondée et conditionnellement résolue		
Finances	31		4	1	20	1	15		7		**48**	**79**
Transports	12	56	1		3	1				1	**62**	**74**
Télécommunications	34		2		1	1	4		2		**10**	**44**
Services	19			2	4	1			6		**13**	**32**
Internet	16		2	2	3		2		1	5	**15**	**31**
Autres secteurs	15		1	3	6	1		1	1		**13**	**28**
Assurances	14		1	2	4	1	1		4		**13**	**27**
Vente/commerce de détail	16		1		1	1		1	1	1	**6**	**22**
Hébergement	16				1		2				**3**	**19**
Professionnels	4		1	2	5						**8**	**12**
Divertissement	3				1		1		2		**4**	**7**
Total	**180**	**56**	**13**	**12**	**49**	**7**	**25**	**2**	**24**	**7**	**195**	**375**

Annexe 1

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 vu 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 exception dont l'organisation s'est prévalue pour retrancher 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 exigé que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels comme condition à l'obtention des biens ou des services.

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 dont elle a la garde ou elle a omis de désigner une personne responsable de surveiller le respect de la *Loi***.**

Transparence : Une organisation a omis de rendre facilement accessibles 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***.**

Annexe 2

Définitions des conclusions et des autres décisions

Au début de l'année 2012, le Commissariat a modifié certaines des définitions des conclusions et des décisions afin qu'elles expriment mieux les résultats de ses enquêtes en vertu de la LPRPDE. Ces nouvelles décisions avaient également pour but de mieux refléter les responsabilités des organisations à rendre des comptes en vertu de la *Loi*.

Les définitions ci-dessous expliquent ce que signifie chaque décision.

Non fondée : L'enquête n'a pas permis de déceler des éléments de preuve donnant à penser qu'une organisation a enfreint la LPRPDE ou de déceler assez d'**éléments de preuve à cette fin.**

Fondée et conditionnellement résolue : Le commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE. L'organisation s'est engagée à mettre en œuvre les recommandations formulées par le commissaire et à faire la démonstration de cette mise en œuvre dans les délais prescrits**.**

Fondée et résolue : Le commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE. L'organisation a démontré qu'elle avait pris des mesures correctives satisfaisantes pour remédier à la situation, soit de sa propre initiative, soit à la suite de recommandations formulées par le commissaire, au moment où la conclusion a été rendue**.**

Fondée : Le commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE**.**

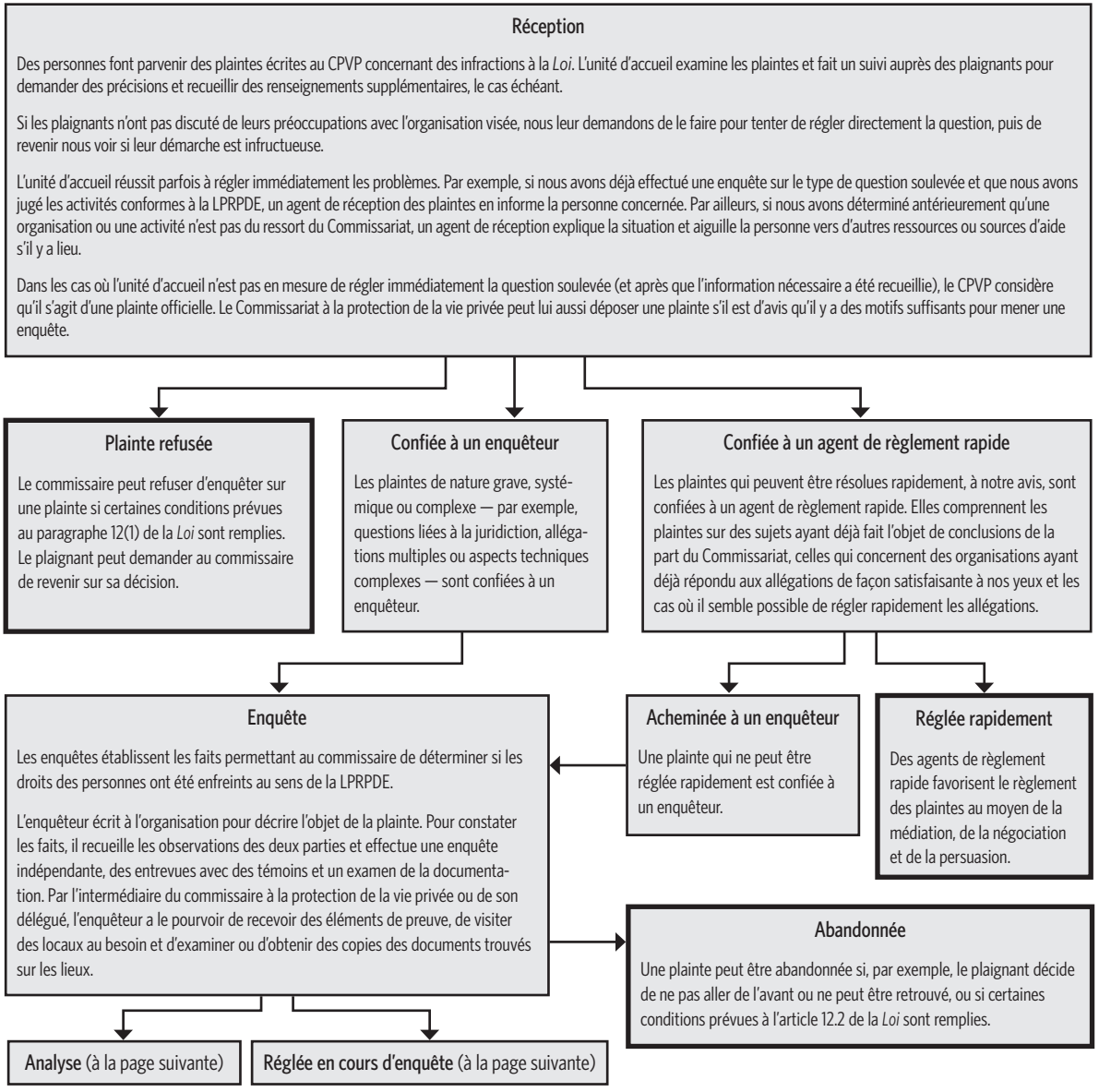
Réglée : Le Commissariat a aidé à négocier une solution satisfaisante pour toutes les parties concernées en cours d'enquête. Le commissaire ne produit pas de rapport**.**

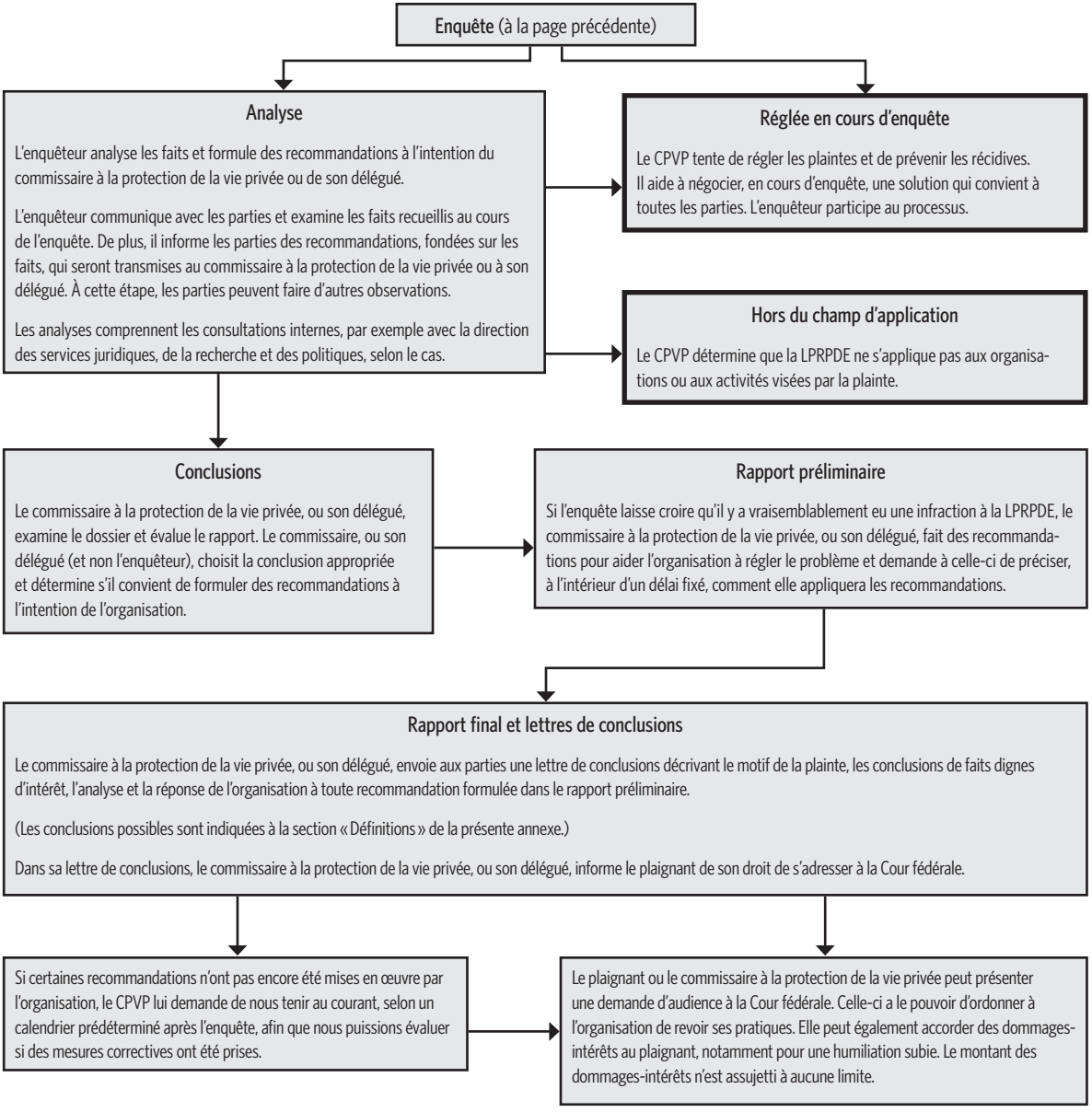
Mettre fin à l'examen : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. À sa discrétion, le commissaire peut mettre fin à l'examen de la plainte pour un motif prévu au paragraphe 12.2(1) de la LPRPDE, à la demande du plaignant ou lorsqu'il a renoncé à la plainte.

Refus d'enquêter : Le commissaire a refusé de procéder à une enquête relative à une plainte parce qu'il était d'avis que le plaignant aurait d'abord dû épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; que la plainte pourrait avantageusement être instruite selon des procédures prévues par le droit fédéral ou le droit provincial; que la plainte n'a pas été déposée dans un délai raisonnable après que son objet a pris naissance, conformément au paragraphe 12(1) de la LPRPDE.

Hors du champ d'application : À la lumière des données préliminaires recueillies, on a déterminé que la LPRPDE ne s'appliquait pas à l'organisation ou à l'activité faisant l'objet de la plainte. Le commissaire ne produit pas de rapport.

Annexe 3 Processus d'enquête




Enquête (à la page précédente)
Analyse
L'enquêteur analyse les faits et formule des recommandations à l'intention du commissaire à la protection de la vie privée ou de son délégué.
L'enquêteur communique avec les parties et examine les faits recueillis au cours de l'enquête. De plus, il informe les parties des recommandations, fondées sur les faits, qui seront transmises au commissaire à la protection de la vie privée ou à son délégué. À cette étape, les parties peuvent faire d'autres observations.
Les analyses comprennent les consultations internes, par exemple avec la direction des services juridiques, de la recherche et des politiques, selon le cas.
Réglée en cours d'enquête
Le CPVP tente de régler les plaintes et de prévenir les récidives. Il aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. L'enquêteur participe au processus.
Hors du champ d'application
Le CPVP détermine que la LPRPDE ne s'applique pas aux organisations ou aux activités visées par la plainte.
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), choisit la conclusion appropriée et détermine s'il convient de formuler des recommandations à l'intention de l'organisation.
Rapport préliminaire
Si l'enquête laisse croire qu'il y a vraisemblablement eu une infraction à la LPRPDE, le commissaire à la protection de la vie privée, ou son délégué, fait des recommandations pour aider l'organisation à régler le problème et demande à celle-ci de préciser, à l'intérieur d'un délai fixé, comment elle appliquera les recommandations.
Rapport final et lettres de conclusions
Le commissaire à la protection de la vie privée, ou son délégué, envoie aux parties une lettre de conclusions décrivant le motif de la plainte, les conclusions de faits dignes d'intérêt, l'analyse et la réponse de l'organisation à toute recommandation formulée dans le rapport préliminaire.
(Les conclusions possibles sont indiquées à la section « Définitions » de la présente annexe.)
Dans sa lettre de conclusions, le commissaire à la protection de la vie privée, ou son délégué, informe le plaignant de son droit de s'adresser à la Cour fédérale.
Si certaines recommandations n'ont pas encore été mises en œuvre par l'organisation, le CPVP lui demande de nous tenir au courant, selon un calendrier prédéterminé après l'enquête, afin que nous puissions évaluer si des mesures correctives ont été prises.
Le plaignant ou le commissaire à la protection de la vie privée peut présenter une demande d'audience à la Cour fédérale. Celle-ci a le pouvoir d'ordonner à l'organisation de revoir ses pratiques. Elle peut également accorder des dommages-intérêts au plaignant, notamment pour une humiliation subie. Le montant des dommages-intérêts n'est assujetti à aucune limite.