

# PROTECTION DE LA VIE PRIVÉE – NOS PRIORITÉS

Réflexions sur les priorités stratégiques du Commissariat  
à la protection de la vie privée du Canada



Commissariat  
à la protection de  
la vie privée du Canada





Commissariat  
à la protection de  
la vie privée du Canada

Le présent document ne présente qu'un petit échantillon du travail accompli en ce qui a trait à nos priorités stratégiques. La version intégrale du rapport, qui recense toutes nos activités, est affichée sur le site Web du Commissariat.



## Table des matières

- 2 Message de la commissaire
- 7  **PRIORITÉ**  
Sécurité publique et protection de la vie privée
- 17  **PRIORITÉ**  
Technologie de l'information et protection de la vie privée
- 25  **PRIORITÉ**  
Intégrité et protection de l'identité
- 35  **PRIORITÉ**  
Renseignements génétiques et protection de la vie privée
- 43 La voie à suivre

# MESSAGE DE LA COMMISSAIRE

L'un des plus grands défis auxquels se heurtent les organismes de réglementation de la vie privée au 21<sup>e</sup> siècle tient aux nouveaux risques d'atteinte à la vie privée – et ils sont légion – qui surgissent la plupart du temps à une vitesse fulgurante sous des formes que nous n'aurions pas pu imaginer il y a seulement quelques années.

En fait, le paysage de la vie privée est en constante évolution et se transforme de façon spectaculaire.

Pour relever ce défi aussi efficacement que possible, le Commissariat a décidé, en 2007, de définir quelques grandes priorités stratégiques autour desquels il articulerait désormais ses travaux.

À la suite de délibérations approfondies, nous avons déterminé nos principaux axes d'intervention en cette époque de changement rapide, à savoir : 1) la technologie de l'information; 2) la sécurité publique; 3) l'intégrité de l'identité; 4) les renseignements génétiques.

Ces priorités nous ont aidés à classer par ordre de priorité les demandes et les revendications reçues par le Commissariat, à élaborer nos plans de travail et à affecter nos ressources aux activités

susceptibles d'avoir le maximum de retombées pour les Canadiens.

## DÉFINITION DE NOS QUATRE PRIORITÉS

Au moment de définir nos priorités stratégiques, nous avons tenu compte de plusieurs critères.

Nous avons évalué plusieurs priorités éventuelles en fonction de leur importance intrinsèque, c'est-à-dire de leur portée nationale ou internationale le cas échéant, de leur urgence relative et de leur pertinence pour les Canadiens.

Nous avons pris en compte le rôle que nous pourrions jouer à l'appui d'une priorité donnée : en déterminant si la priorité relevait ou non de la compétence fédérale, si elle concordait ou non avec notre mandat et si elle était pertinente pour les secteurs public et privé, quel était le type de

leadership qui s'imposait et quelle valeur ajoutée la contribution du Commissariat pouvait apporter.

Enfin, nous nous sommes penchés sur les aspects pratiques, par exemple la possibilité de véritables retombées, la capacité d'obtenir des résultats dans un délai de trois à cinq ans, les investissements passés dont nous pourrions tirer parti par la suite et les partenaires avec lesquels nous pourrions nous associer.

À l'issue de cette démarche, nous nous sommes entendus sur les quatre priorités suivantes, qui ont une très grande incidence sur la vie privée :

- > Sécurité publique et protection de la vie privée
- > Technologie de l'information et protection de la vie privée
- > Intégrité et protection de l'identité
- > Renseignements génétiques et protection de la vie privée

À l'époque, nous voyions dans chacun de ces domaines la possibilité de faire évoluer les normes sociales et les modèles fonctionnels de manière à avoir des retombées considérables sur le droit à la vie privée.

Nous prévoyions alors que la soif de renseignements personnels connaîtrait une croissance exponentielle et que la quête d'innovation progresserait à la vitesse de l'éclair dans le monde entier.

Nous entrevoyions la possibilité, pour le Commissariat, de participer activement aux débats publics requis pour soulever en temps utile les préoccupations en matière de vie privée. Nous avons entrepris d'encourager les institutions

gouvernementales et les organisations du secteur privé à mettre en place les mesures de protection nécessaires pour atténuer les risques d'atteinte à la vie privée sur ces fronts. Nous avons favorisé l'innovation et le progrès responsable d'une manière qui protégerait le droit à la vie privée et, à terme, nous permettrait de gagner et de conserver la confiance des Canadiens.

### **AFFECTATION DES RESSOURCES ET QUESTIONS PRIORITAIRES**

Nous avons créé, pour chaque priorité, un groupe de travail composé d'employés issus des différentes directions du Commissariat. Les quatre groupes de travail se sont réunis régulièrement pour discuter de questions pertinentes, mettre l'information en commun et apprendre auprès de spécialistes de l'extérieur.

En articulant notre travail en fonction de ces quatre priorités, nous avons pu affecter nos ressources de manière à maximiser les retombées positives pour les Canadiens.

Par exemple, cette démarche a guidé nos décisions concernant les enquêtes à amorcer, les vérifications relatives au respect de la vie privée ou les examens des évaluations des facteurs relatifs à la vie privée à privilégier, les projets de recherche à entreprendre ou à financer dans le cadre de notre Programme des contributions, les documents d'orientation à publier et les activités de sensibilisation du public et des intervenants sur lesquelles nous concentrer.

Elle a également renforcé notre capacité sur ces fronts, ce qui nous a donné une longueur d'avance dans notre travail sur les politiques, nos avis au Parlement, nos conseils aux entreprises et aux

citoyens, ainsi que notre capacité de prévoir les questions émergentes et d'y réagir.

### **INCIDENCE VITALE**

À l'heure actuelle, diverses menaces d'envergure pèsent sur la vie privée des Canadiens.

En ce qui a trait à nos quatre priorités stratégiques, je suis fière de constater que nous avons accompli des progrès considérables au chapitre de la sensibilisation du public à ces nouveaux problèmes, tant dans le secteur public que privé.

Nous avons utilisé les outils de conformité et d'éducation dont nous disposons pour encourager les institutions gouvernementales et les organisations du secteur privé à se doter de politiques et de pratiques plus respectueuses de la vie privée.

Grâce à des efforts proactifs en matière de recherche, nous avons également acquis de nouvelles connaissances et renforcé notre capacité interne sur ces questions clés en matière de vie privée – convaincus que nous étions de la nécessité de prendre le temps de bien comprendre les changements qui influent sur la vie privée et de rester à l'avant-garde au lieu de nous laisser distancer.

### **ÉTABLISSEMENT DE LIENS**

Au moment d'entreprendre cette démarche, nous étions nombreux à voir ces quatre priorités comme des domaines très distincts. Toutefois, les nombreux liens qui les unissent se sont dévoilés au cours des dernières années.

Les quatre domaines prioritaires ont été balayés par le tsunami des mégadonnées. Qu'il s'agisse de la collecte massive et du regroupement des

renseignements sur les voyages et la sécurité, du choix des amis, des liens, des gazouillis, des mentions « j'aime » ou « je n'aime pas » recueillis dans les médias sociaux, des tendances liées aux habitudes d'achat en ligne des consommateurs et des comportements de recherche dans le Web, des analyses de la séquence du génome entier portant sur des populations dans leur ensemble – nous observons un changement important dans la façon dont les renseignements personnels sont recueillis, utilisés et fondamentalement compris.

Les renseignements personnels sont devenu la monnaie d'échange qui alimente ce nouveau phénomène.

Dans un article paru dans *Foreign Affairs*, Kenneth Cukier et Viktor Mayer-Schöenberger résument le phénomène en ces mots :

*Les mégadonnées sont appelées à remodeler la façon dont nous vivons, travaillons et pensons. Une prépondérance de corrélations remet en question une vision du monde reposant sur l'importance de la relation de cause à effet. La possession de connaissances, qui se traduisait autrefois par la compréhension du passé, est en voie de signifier la capacité de prévoir l'avenir. Il ne sera pas facile de relever les défis inhérents aux mégadonnées. Il s'agit purement et simplement de la prochaine étape du débat intemporel concernant la meilleure façon de comprendre le monde [traduction]<sup>1</sup>.*

Tout en reconnaissant les formidables avantages sociaux qui pourraient découler de cette quête de

---

<sup>1</sup> Kenneth Cukier et Viktor Mayer-Schöenberger. « The Rise of Big Data : How It's Changing the Way We Think About the World ». *Foreign Affairs*, 92 (2013), p. 28-40.

nouvelles formes de connaissance, il m'incombe, en tant que commissaire à la protection de la vie privée du Canada, de cerner les risques d'atteinte à la vie privée en jeu et de travailler à les atténuer au nom des Canadiens.

Le Commissariat s'efforce de favoriser des avancées responsables, tout en empêchant les renseignements personnels des Canadiens d'être utilisés de façon abusive dans la course rapide à la recherche de profits ou d'opportunisme.

Avec le temps, j'en suis arrivée à voir ces questions essentiellement comme des questions éthiques concernant notre compréhension du monde qui nous entoure, le respect que nous portons au droit à l'autonomie et à la dignité des individus, et le type de société dans laquelle nous voulons vivre.

## CONCLUSION

Il y a plusieurs années que nous avons défini les priorités stratégiques et mon mandat arrive à son terme. Le moment est maintenant venu de dresser l'état des lieux.

Avec le recul, on peut se demander si ces quatre priorités étaient les bonnes, ce que nous avons appris à leur sujet et si le Commissariat a fait une différence sur ces fronts. Si nous devons redéfinir des priorités aujourd'hui, choisirions-nous les mêmes ou ferions-nous des choix différents?

Nous estimons que l'initiative des priorités stratégiques est une réussite à tous les égards.

Dans les pages qui suivent, nous mettrons en lumière quelques-unes de nos réalisations qui ont eu une réelle incidence sur le droit des Canadiens à la vie privée.

Je quitterai le Commissariat à la protection de la vie privée du Canada à la fin de 2013, après dix ans à la barre de l'organisme. Je formule ces observations dans l'espoir qu'elles lanceront des idées utiles pour protéger la vie privée au cours des années à venir.

La personne qui me remplacera en tant que commissaire partira d'une page blanche et il lui reviendra de déterminer les priorités pour le prochain mandat. J'ai bon espoir que le Commissariat et ses spécialistes extrêmement compétents continueront de s'appuyer sur la solide assise que nous avons déjà mise en place, et ce, quels que soient les défis que l'avenir leur réserve.

Enfin, j'aimerais profiter de l'occasion pour remercier mes employés pour le dévouement et la passion dont ils font preuve afin de protéger la vie privée. Ils se font un devoir d'atteindre les normes d'excellence et d'adopter le comportement éthique auxquels les Canadiens s'attendent de la part des fonctionnaires. Je les remercie du travail exceptionnel accompli au fil des ans en ce qui a trait à nos quatre priorités stratégiques.

Nous en avons fait, du chemin!



La commissaire à la protection de la vie privée du Canada,  
**JENNIFER STODDART**



**D**  
Gates/Portes



**i** Information

- ↓ ↗ P
- ↓ ↗
- ↓ ↗

Ground Level Re... sée

**Priority Check-in**  
Enregistrement prioritaire



PRIORITÉ

# SÉCURITÉ PUBLIQUE ET PROTECTION DE LA VIE PRIVÉE

## COMMENT TOUT A COMMENCÉ

Les attentats terroristes perpétrés contre les États-Unis en septembre 2001 ont donné lieu à un renforcement considérable des mesures de sécurité nationale à la grandeur de l'Amérique du Nord, notamment à la frontière canado-américaine.

Compte tenu de la montée en flèche des capacités technologiques, les autorités cherchent à tenir en échec le terrorisme et la criminalité en surveillant ce que les gens disent et font, en repérant leurs comportements suspects, voire en prévoyant leurs intentions.

D'entrée de jeu, le Commissariat a pris conscience du fait que le droit à la vie privée, bien qu'il s'agisse d'un droit fondamental, n'est pas absolu. Il doit être exercé en lien avec d'autres droits fondamentaux – en l'espèce, le droit de vivre sa vie en sécurité à l'abri de la menace de préjudices.

La sécurité publique et la protection de la vie privée ne sont pas incompatibles. En fait, il faut les intégrer et les adapter afin qu'elles puissent continuer de coexister dans une société libre et démocratique.

## CE QUE NOUS AVONS OBSERVÉ

Nos travaux dans le domaine ont révélé une nette augmentation de la capacité des organismes de sécurité publique de recueillir et de stocker de grandes quantités de renseignements personnels.

Les avancées technologiques ont donné naissance à une nouvelle génération d'appareils mobiles, de télécapteurs, de caméras haute résolution et de logiciels d'analyse qui ont tous révolutionné les techniques de surveillance.

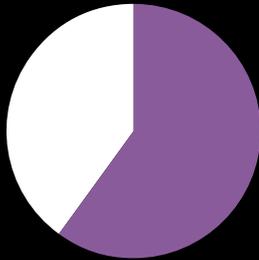
La technologie a aussi permis la mise au point d'un vaste éventail de bases de données renfermant des



## LA VIE PRIVÉE EN CHIFFRES

Dans un sondage mené à la fin de 2012 par l'Association d'études canadiennes, 60 % des répondants ont affirmé

ne pas être prêts à renoncer à certaines libertés civiles pour combattre le terrorisme au pays.



**60 %**  
ne sont pas prêts à renoncer à leurs libertés civiles

Terrorism and Counter terrorism: Knowledge, Fears and Perceived Causes, Association d'études canadiennes, décembre 2012  
<http://www.acs-aec.ca/en/> (en anglais seulement).

renseignements personnels plus imposantes que jamais et de plus en plus perfectionnées.

D'énormes quantités de renseignements personnels – par exemple les données relatives au trafic de communications, aux opérations financières et aux itinéraires de voyage par avion – sont recueillies, communiquées, appariées et analysées à des fins de sécurité publique. Et tout cela a lieu à la vitesse de la lumière.

Le Commissariat a fait valoir que les autorités chargées de la sécurité publique doivent répondre, dans une juste mesure, des pouvoirs considérables qui leur sont conférés.

En outre, elles doivent les exercer en respectant les droits fondamentaux et les valeurs canadiennes. Sans ces balises, l'assise même de notre société libre et démocratique – la confiance entre l'État et ses citoyens – serait menacée.

### CE QUE NOUS AVONS ACCOMPLI

Au lieu d'examiner chaque nouvelle mesure de sécurité publique au moment de son introduction, nous avons adopté une approche plus exhaustive, équilibrée, intégrée et, à terme, efficace, en définissant la sécurité publique et la protection de la vie privée comme un domaine prioritaire.

Nous avons estimé que notre rôle consistait à nous assurer que les nouvelles mesures de sécurité publique, malgré leur importance dans ce contexte moderne, ne portent pas indûment atteinte au droit à la vie privée.

Nous n'avons pas essayé de mettre fin aux initiatives en place. Nous nous sommes plutôt efforcés

d'atténuer leurs répercussions négatives éventuelles sur la vie privée en posant des questions, en vérifiant les hypothèses et en procédant à un examen critique des enjeux.

Plus précisément, nos travaux ont jeté une lumière nouvelle sur les initiatives de sécurité publique en incitant les ministères à faire preuve d'une transparence et d'une responsabilité accrues. Nous avons aussi aidé les Canadiens à mieux comprendre les conséquences des mesures de sécurité sur leur vie privée.

Parallèlement, nous avons fourni de l'information aux décideurs et aux parlementaires et nous les avons épaulés en les sensibilisant aux risques d'atteinte à la vie privée susceptibles de découler des mesures législatives proposées aux fins de la sécurité publique. Nous sommes convaincus que nos commentaires ont été appréciés et soigneusement examinés, et qu'ils ont permis, à terme, la prise de décisions plus éclairées.

Dans la plupart des cas, nous estimons que les Canadiens ont bénéficié, au final, d'une approche en matière de sécurité publique plus respectueuse de la vie privée.

Voici quelques exemples de nos activités.

## Une question de confiance

En 2010, nous avons publié un document de référence intitulé *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21<sup>e</sup> siècle*.

Cette publication propose un cadre analytique pour aider les parlementaires, les décideurs et les

concepteurs de programmes à intégrer la sécurité publique et la protection de la vie privée.

Après avoir fait état des hypothèses et des principes sous jacents, elle définit les contrepoids qui permettent de prendre des décisions éclairées concernant toute nouvelle initiative susceptible de porter atteinte à la vie privée.

Avant que les autorités dévoilent une nouvelle mesure de renforcement de la sécurité publique susceptible de porter atteinte à la vie privée, nous les encourageons à se poser quatre questions : L'initiative est-elle vraiment nécessaire? Permettra-t-elle d'atteindre l'objectif visé? Les atteintes à la vie privée susceptibles d'en découler seront-elles proportionnées par rapport aux avantages escomptés? Existe-t-il des solutions de rechange moins intrusives?

## Scanneurs corporels dans les aéroports

La plupart des voyageurs qui fréquentent les aéroports canadiens connaissent les scanneurs qui peuvent saisir des images du corps entier pour détecter les armes non métalliques, les explosifs ou d'autres menaces pour la sécurité aérienne.

La vie privée des voyageurs est mieux protégée grâce aux consultations menées par l'Administration canadienne de la sûreté du transport aérien (ACSTA) auprès du Commissariat.

En effet, l'ACSTA a adopté plusieurs des recommandations que nous avons formulées après avoir examiné son évaluation des facteurs relatifs à la vie privée, ce qui l'a incitée à mettre en place des

améliorations visant à mieux protéger la vie privée des voyageurs.

Par exemple, les voyageurs ont le droit d'opter pour une fouille par palpation au lieu d'un scannage corporel. Les scanners sont utilisés uniquement comme mesure secondaire, lorsque l'on a identifié une menace précise. Qui plus est, les images sont supprimées une fois qu'un responsable a confirmé l'absence de menace.

En 2011, nous avons mené une vérification et confirmé que l'image ne peut être reproduite et qu'elle est détruite de façon définitive une fois que le voyageur a quitté l'aire de scannage. Nous avons aussi formulé des recommandations supplémentaires pour accroître encore davantage la protection de la vie privée.

Le Commissariat a recommandé l'adoption d'un logiciel de reconnaissance automatisée d'objectifs, qui crée des représentations schématiques (bonshommes-allumettes) des personnes scannées.

En 2013, le gouvernement fédéral a annoncé l'adoption de ce logiciel.

## Initiatives se rapportant à la frontière canado-américaine

Les gouvernements du Canada et des États-Unis ont mis en place l'initiative de la sécurité du périmètre Canada-États-Unis, qui vise à renforcer la sécurité et à faciliter le commerce le long de notre frontière commune. Le premier ministre Stephen Harper et le président américain Barack Obama ont signé, en 2011, la déclaration intitulée *Par-delà la frontière*.

Le Commissariat a insisté sur le fait que toutes les initiatives découlant de l'entente doivent intégrer et respecter véritablement le droit à la vie privée conformément aux attentes des Canadiens.

Nous avons participé aux consultations publiques menées par le gouvernement et formulé une série de recommandations à l'égard des risques d'atteinte à la vie privée découlant des différents éléments du modèle de sécurité du périmètre.

Comme nous l'avons expliqué dans notre mémoire, les Canadiens ont des attentes élevées en matière de vie privée et adhèrent fortement au principe de protection des renseignements personnels. Compte tenu des points sensibles concernant les renseignements personnels et la souveraineté, nous sommes portés à croire que toute tentative pour s'écarter de ces normes éclipserait rapidement le débat public sur les plans d'action.

Nous avons souligné que l'échange de renseignements doit absolument se limiter aux éléments précis des renseignements personnels qui sont réellement nécessaires, donner lieu à une utilisation et une communication uniquement à des fins très précises et faire l'objet de mesures de protection et de surveillance rigoureuses.

Enfin, nous avons aussi fortement recommandé d'évaluer les facteurs relatifs à la vie privée des différentes initiatives découlant du plan d'action *Par-delà la frontière* qui portent sur les renseignements personnels.

Le plan d'action du Canada et des États-Unis sur la sécurité du périmètre a été rendu public à l'issue de ces consultations. Nous avons noté que

Have Identification and  
Documentation Ready

Ayez vos papiers  
d'identité et vos documents  
à portée de la main

**Moving?**  
Automatic  
Load Deck

**\$19.95**

ARREY

STOP

Stop until  
vehicle  
ahead is  
cleared

**U-HAUL**

RENT EQUIPMENT • LOWEST COST

Gentle-Ride V...



## Le reste de l'iceberg

Nous ne présentons ici qu'une partie des activités menées par le Commissariat en lien avec la priorité stratégique Sécurité publique et protection de la vie privée. Vous trouverez, sur notre page Web spéciale, une liste complète des initiatives visées, y compris l'examen des fichiers inconsultables de la Gendarmerie royale du Canada (GRC), des bases de données opérationnelles de la GRC, des pratiques de retrait des renseignements personnels de certaines institutions fédérales, de l'Administration canadienne de la sûreté du transport aérien, des opérations liées au passeport canadien et du Programme de protection des passagers (mieux connu sous le nom de « Liste de personnes interdites de vol »). D'autres travaux portaient sur les questions de protection de la vie privée soulevées par les modifications apportées aux politiques touchant la frontière canada-américaine ainsi que par le renforcement des mesures de la protection de la vie privée pour les utilisateurs du permis de conduire Plus et des certificats de statut d'Indien. Nous avons aussi examiné les efforts déployés par le gouvernement pour adopter une législation sur l'accès légal.

les deux pays s'engageaient alors à respecter leur souveraineté mutuelle et le droit de l'autre partie de prendre des décisions et d'évaluer le risque de façon indépendante. En outre, le plan d'action prévoyait que chaque pays tiendrait des bases de données distinctes.

C'est avec plaisir que nous constatons que les ministères et organismes canadiens consultent régulièrement le Commissariat et lui soumettent des évaluations des facteurs relatifs à la vie privée aux fins d'examen et de recommandations.

Nous examinons à l'heure actuelle sept évaluations des facteurs relatifs à la vie privée se rapportant au plan d'action et nous avons mené à bien 12 examens similaires à ce jour.

## Vérification du CANAFE

Afin de détecter et de décourager le recyclage des produits de la criminalité et le financement des activités terroristes, ainsi que de faciliter les enquêtes et les poursuites, la loi oblige des dizaines de milliers d'entreprises exerçant leurs activités au Canada à recueillir des renseignements personnels sur leurs clients et à signaler certaines opérations financières au Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).

En 2009, nous avons effectué une vérification pour déterminer si le CANAFE avait mis en place des mécanismes de contrôle appropriés afin de protéger les renseignements personnels et si les procédures et les pratiques dont il s'était doté pour gérer cette information étaient conformes à la

*Loi sur la protection des renseignements personnels.* Les Canadiens doivent avoir l'assurance que leurs renseignements personnels sont gérés comme il se doit dans le cadre de mécanismes de contrôle bien établis. Tous les ministères sont tenus de protéger les renseignements personnels, mais cette exigence est encore plus rigoureuse dans le cas d'organisations comme le CANAFE.

Nous avons constaté que, même si le CANAFE disposait de systèmes appropriés pour recueillir et gérer les renseignements personnels et financiers, certaines entités déclarantes étaient beaucoup trop enclines à communiquer des renseignements, parfois pour des raisons à peine valables.

Nous avons remarqué que le CANAFE reçoit et conserve des renseignements qui ne se limitent pas à l'information se rapportant directement à ses programmes et activités en cours. Il faut renforcer les mécanismes de contrôle en place, notamment l'examen préliminaire et le suivi permanent des rapports, de manière à limiter les fonds de renseignements du CANAFE.

## Accès légal

Le Commissariat comprend les défis auxquels se heurtent les autorités chargées de l'application de la loi dans la lutte contre la cybercriminalité à une époque où les technologies des communications évoluent rapidement. Il comprend aussi qu'elles doivent moderniser leurs tactiques et leurs outils en conséquence.

Les propositions du gouvernement fédéral concernant la question de l'accès légal nous ont toutefois grandement inquiétés.

Le projet de loi C-30 qui a été présenté par le gouvernement aurait permis aux organismes chargés de l'application de la loi d'avoir accès sans mandat aux renseignements des abonnés, par exemple l'adresse IP. Au dire des partisans du projet de loi, cette information était de la même nature que celle qui figure dans un annuaire téléphonique.

Les technologues du Commissariat ont examiné le degré d'atteinte à la vie privée associé aux renseignements que le projet de loi se proposait de rendre accessibles aux autorités policières.

Dans le rapport produit à la suite d'une analyse technique qui est affiché sur notre site Web, nous démontrons qu'une adresse IP peut, en fait, être un point de départ permettant de brosser le portrait des activités en ligne d'une personne, y compris les services en ligne auxquels elle est abonnée, ses intérêts personnels en fonction des sites Web consultés, les organisations auxquelles elle appartient et même son emplacement physique.

Les Canadiens ont accueilli très défavorablement le projet de loi C-30 et ont dit craindre qu'il n'ait des conséquences négatives importantes sur leur droit fondamental à la vie privée.

Nous avons été heureux de constater que le gouvernement donnait suite à ces préoccupations lorsqu'il a annoncé, en février 2013, son intention de ne pas donner suite au projet de loi C-30.

## Mémoires au Parlement

Au fil des ans, les représentants du Commissariat ont témoigné devant des comités parlementaires pour faire part de nos points de vue sur un grand

nombre de mesures législatives et d'examen touchant la sécurité publique, par exemple la législation antiterroriste canadienne. Nous avons aussi exprimé notre opinion en témoignant et en présentant des mémoires dans le cadre de commissions d'enquête fédérales, par exemple la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India.

### **CE QUE CELA SIGNIFIE POUR VOUS**

La sécurité et la protection de la vie privée ne sont pas incompatibles. Elles peuvent bel et bien coexister. En fait, nous estimons qu'elles doivent se renforcer mutuellement pour protéger la société démocratique dans laquelle nous vivons.

Depuis qu'il s'agit de l'une de nos priorités stratégiques, nous nous efforçons de rallier les législateurs et les organismes chargés de la sécurité publique à cette approche plus équilibrée.

Nos travaux à l'appui de cette priorité stratégique ont renforcé nos propres réflexions sur ces enjeux.

Ils ont accru notre crédibilité auprès des organismes chargés de la sécurité publique, des gouvernements et du public. Nous avons ainsi pu établir des axes de communication essentiels avec ces intervenants pour nous assurer que les préoccupations en matière de vie privée demeurent à l'avant-plan.

Nos efforts ont montré que la relation entre les organismes chargés de la sécurité publique et les personnes qu'ils protègent repose sur la confiance. De façon générale, les gens sont prêts à accepter certains inconvénients et à faire des sacrifices sur le

plan de la vie privée, pourvu que l'État fasse preuve de transparence, de responsabilité et d'intégrité.

Pour l'essentiel, il s'agit de traiter les renseignements personnels des Canadiens avec le soin et le respect extrêmes qu'ils méritent.

### **PERSPECTIVES D'AVENIR**

S'il est difficile aujourd'hui de renforcer le droit à la vie privée face aux impératifs de la sécurité publique, il serait illusoire de penser que les choses seront plus simples à l'avenir.

La cybercriminalité et le cyberespionnage font peser de nouvelles menaces graves sur l'infrastructure numérique sur laquelle repose notre vie quotidienne, dont la possibilité d'atteintes à la vie privée d'une envergure stupéfiante.

Afin de faire échec à ces menaces, les autorités ont de plus en plus recours à la surveillance, aux analyses et à d'autres technologies pour recueillir, stocker, extraire et communiquer des renseignements personnels, souvent en échappant à la portée des organismes de supervision.

Mais nous espérons qu'il sera possible d'appliquer de façon utile un cadre fondé sur des principes et axé sur les valeurs chères aux Canadiens dans une société libre et démocratique pour favoriser l'intégration des mesures de protection de la vie privée et des objectifs en matière de sécurité publique et nationale.

•REC





# TECHNOLOGIE DE L'INFORMATION ET PROTECTION DE LA VIE PRIVÉE

## COMMENT TOUT A COMMENCÉ

Au moment de choisir les priorités stratégiques, la technologie de l'information s'est imposée d'emblée parce qu'un très grand nombre d'enjeux liés à la protection de la vie privée renferment un volet technologique.

En cette ère numérique, il est impossible d'analyser de manière approfondie les enjeux liés à la protection de la vie privée sans comprendre l'aspect technologique sous-jacent.

La technologie évolue à un rythme effarant et les conséquences des technologies naissantes sur la vie privée ne sont pas toujours apparentes sur le coup.

Notre mission consistait donc à repérer, de façon proactive, les nouvelles avancées technologiques et

à faire de notre mieux pour prendre une longueur d'avance. Il nous fallait acquérir la capacité interne nécessaire pour analyser et comprendre les leviers du marché et leur incidence sur la vie privée. C'est seulement à ce stade que nous pourrions nous prononcer de façon crédible sur les risques d'atteinte à la vie privée connexes et inciter les organisations et les individus à prendre les mesures nécessaires pour les atténuer.

## CE QUE NOUS AVONS OBSERVÉ

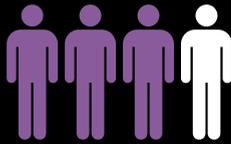
Que ce soit dans les domaines de l'éducation, de la santé, de l'administration publique ou du commerce, ou simplement dans la sphère privée, la technologie est omniprésente. Auparavant, nous ne sortions jamais sans notre porte-monnaie. Aujourd'hui, nombre de Canadiens ne peuvent plus se passer de leur téléphone intelligent ou de leur tablette.

## LA VIE PRIVÉE EN CHIFFRES

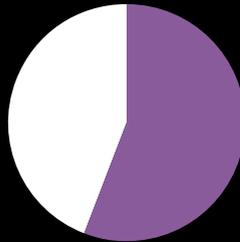
Selon un sondage mené en 2012 par le Commissariat, trois Canadiens sur quatre – et 92 % des jeunes – utilisent un appareil mobile, par exemple un téléphone cellulaire, un téléphone intelligent ou une tablette.

# Toutefois, seulement 56 % utilisent un mot de passe pour le verrouiller

et une proportion plus faible encore ajustent les paramètres de l'appareil ou des applications afin de limiter la quantité de renseignements personnels qui sont partagés avec d'autres.



**3 sur 4**  
utilisent un  
appareil mobile



**56 %**  
utilisent un  
mot de passe

Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée, rapport final préparé pour le Commissariat à la protection de la vie privée du Canada par Phoenix SPI 2013.  
[http://www.priv.gc.ca/information/por-rop/2013/por\\_2013\\_01\\_f.asp](http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_f.asp)

Les appareils technologiques deviennent non seulement plus portatifs, mais aussi plus puissants.

Ils permettent d'exécuter davantage de fonctions pour lesquelles il fallait auparavant utiliser plusieurs appareils différents. C'est ainsi qu'une foule de renseignements personnels sont maintenant stockés dans de minuscules appareils que l'on peut facilement perdre ou se faire voler, ce qui constitue de toute évidence un risque d'atteinte à la vie privée.

En outre, le fait que de nombreux employés ont constamment sur eux un téléphone intelligent fourni par leur employeur accroît le risque d'atteinte à la sécurité des renseignements personnels stockés dans les dossiers des entreprises ou des gouvernements.

On observe également d'autres formes de convergence des renseignements, par exemple sur une plateforme en ligne unique comme Facebook ou par un fournisseur de services unique comme Google. Dans ce type d'environnement, la capacité des utilisateurs de maîtriser leurs renseignements personnels s'éffrite.

Qui plus est, à mesure qu'elle devient « plus intelligente », la technologie se fond dans le décor. Certes, c'est agréable pour les utilisateurs, mais il devient aussi plus difficile de savoir quels renseignements personnels sont recueillis et utilisés.

En réalité, entre les systèmes GPS, les technologies d'identification par radiofréquence (RFID), les logiciels de suivi en ligne qui peuvent analyser l'historique de recherche et l'équipement qui peut lire des indicateurs biométriques, le citoyen ordinaire transmet sans le savoir d'énormes quantités de renseignements personnels.

## CE QUE NOUS AVONS ACCOMPLI

Compte tenu du prodigieux éventail de questions liées à la technologie, nous avons pris conscience de l'importance d'acquérir plus de connaissances sur le sujet.

Nous avons créé un laboratoire technologique spécialisé, tenu des consultations publiques sur certaines nouvelles tendances et réalisé une étude internationale sur les nouvelles technologies de l'information.

Les connaissances que nous avons acquises étaient essentielles pour nous permettre de collaborer avec les organisations sur un pied d'égalité en ce qui a trait aux aspects hautement technologiques et d'adopter des positions crédibles et nuancées à cet égard.

Au fil des ans, nous avons tiré parti de nos connaissances sur les enjeux technologiques pour élaborer des documents d'orientation et de sensibilisation ciblés. Ces connaissances nous ont également été utiles dans le cadre de nos enquêtes et de nos vérifications, ainsi que dans l'exercice des responsabilités nous incombant en vertu de la nouvelle loi canadienne anti-pourriel.

Voici quelques exemples de nos activités.

### Direction de l'analyse des technologies

Nous avons créé la Direction de l'analyse des technologies, qui compte sur des employés spécialisés et un laboratoire pour effectuer les analyses techniques nécessaires à l'appui des activités du Commissariat.

Nos technologues peuvent notamment aider nos enquêteurs à évaluer les aspects techniques d'une plainte, par exemple les options de confidentialité ou les paramètres par défaut, certaines caractéristiques des services en ligne, l'efficacité des mesures de sécurité ou les pratiques alléguées de suppression des renseignements.

Le laboratoire d'analyse des technologies constitue également un banc d'essais initiaux pour la recherche portant sur de nouvelles applications et d'autres technologies naissantes pouvant avoir une incidence sur la vie privée, même avant qu'elles fassent l'objet d'une plainte pour atteinte à la vie privée.

Nos technologues ont également apporté un soutien technique pour aider le Commissariat à se préparer à assumer les nouvelles responsabilités qui lui incomberont par suite de l'adoption de la loi canadienne anti-pourriel. Le Commissariat veillera à l'application de cette loi conjointement avec le Bureau de la concurrence et le Conseil de la radiodiffusion et des télécommunications canadiennes, mais son rôle consistera plus précisément à surveiller la collecte non autorisée de renseignements personnels, soit par le prélèvement d'adresses de courriel ou l'installation de logiciels espions sur l'ordinateur de particuliers.

### Réseautage social

La popularité fulgurante des réseaux sociaux a donné lieu à une enquête sur les pratiques de protection de la vie privée de Facebook.

Par suite de notre enquête, le géant du réseautage social a modifié sa plateforme pour empêcher toute application d'avoir accès à des renseignements sans le consentement préalable explicite de l'utilisateur.

## Le reste de l'iceberg

Nous ne présentons ici qu'une partie des activités menées par le Commissariat en lien avec la priorité stratégique Technologie de l'information et protection de la vie privée. Vous trouverez sur notre site Web une liste complète de nos activités, par exemple, une description de notre étude consacrée aux fuites sur Internet et de notre projet d'inspection approfondie des paquets, ainsi que le mémoire au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) sur ce type d'inspection. Vous y trouverez également notre document d'orientation sur les jeux vidéo et toute une gamme de fiches d'information sur une panoplie de sujets, des témoins jusqu'au détournement des renseignements personnels en ligne. Mentionnons aussi plusieurs enquêtes où la technologie de l'information constituait un enjeu clé.

En réponse à une autre préoccupation concernant la transparence, Facebook a accepté de donner aux utilisateurs davantage d'information sur la protection de la vie privée et d'améliorer ses outils à cet égard.

Cette enquête revêtait une grande importance pour plusieurs raisons. À l'échelle mondiale, nous étions la première autorité de protection des renseignements personnels à mener une vaste enquête sur les politiques et les pratiques de Facebook au chapitre de la protection de la vie privée. Nous avons établi que les sites de réseautage social soulevaient des enjeux fondamentaux liés à la protection de la vie privée et que ces sites devraient s'acquitter de leurs obligations en la matière – et rendre des comptes.

Des millions d'utilisateurs du monde entier ont profité des changements que Facebook a accepté d'apporter à ses pratiques de protection de la vie privée.

Notre enquête sur Facebook a également envoyé un message clair aux organisations en ligne :

Internet n'est pas un territoire où tout est permis dans le domaine de la vie privée et les autorités de protection des renseignements personnels les ont à l'œil.

Au fil des ans, nous avons mené d'autres enquêtes sur Facebook.

Nous avons également examiné des enjeux liés à la protection de la vie privée sur d'autres sites de réseautage social, dont Nexopia, qui s'adresse expressément aux jeunes.

## Infonuagique

Les entreprises, les particuliers et même les gouvernements se tournent de plus en plus vers les services d'infonuagique, qui peuvent s'avérer une façon pratique de stocker et de traiter de grandes quantités d'information sans les maux de tête habituellement liés à la gestion d'une infrastructure de TI.

Toutefois, l'infonuagique peut aussi comporter des risques d'atteinte à la vie privée, simplement en raison de l'immensité des données stockées sur des serveurs se trouvant dans différentes régions du monde.

Conscients de la popularité croissante des services d'infonuagique et de ses répercussions importantes sur la vie privée, nous avons mis au point plusieurs outils d'information à l'intention de divers groupes. Une fiche d'information s'adressant au grand public fournit des renseignements généraux sur le sujet, tandis qu'un document d'orientation plus spécialisé, que nous avons produit en collaboration avec nos homologues de l'Alberta et de la Colombie-Britannique, aide les petites et moyennes entreprises à mieux comprendre l'infonuagique et les responsabilités en matière de vie privée qui leur incombent lorsqu'elles y exercent des activités.

## Protection de la vie privée et appareils mobiles

Les appareils mobiles renferment plus de renseignements personnels que jamais auparavant. Lorsque les gens sont connectés à Internet, en particulier s'ils ont activé les fonctions de localisation, ils s'exposent à un risque croissant de surveillance exhaustive.

En 2013, nous avons collaboré avec l'autorité néerlandaise de protection des données dans le cadre d'une enquête sans précédent portant sur les pratiques de protection des renseignements personnels de WhatsApp, un développeur californien d'une application mobile de messagerie multiplateforme. Notre enquête portant sur la plateforme de messagerie mobile de l'entreprise a mis en évidence de nombreux risques d'atteinte à la sécurité des renseignements personnels.

WhatsApp s'est attachée à remédier aux défaillances relevées. Par exemple, donnant partiellement suite à notre enquête, elle a ajouté le chiffrement à son service de messagerie mobile et renforcé sa procédure d'authentification dans la dernière version de son application.

En 2012, nous avons fait équipe avec nos homologues de la Colombie-Britannique et de l'Alberta pour publier, à l'intention des développeurs d'applications mobiles, un document d'orientation donnant des conseils sur la responsabilité juridique, la transparence et la justification de la collecte de renseignements personnels. Ce document fait aussi état de l'obligation d'obtenir un consentement valable avant de recueillir de l'information, ce qui s'avère particulièrement difficile lorsque les utilisateurs lisent en diagonale une politique de confidentialité affichée en petits caractères sur un écran minuscule.

Nous avons également lancé un projet de recherche pour examiner les enjeux liés à la protection de la vie privée se rapportant aux paiements mobiles. Nul doute que ce type de paiement révolutionnera la façon dont les Canadiens paient les biens et services.

## Données Wi-Fi recueillies par Google

En 2010, une enquête menée par le Commissariat a révélé que Google contrevenait à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en recueillant de façon inappropriée des renseignements personnels sur des réseaux sans fil non sécurisés un peu partout au pays.

Pendant plusieurs années, les véhicules de Google qui photographiaient des quartiers pour son service de cartes Street View ont également recueilli des données transmises sur des réseaux sans fil non sécurisés aménagés dans des domiciles et des entreprises à la grandeur du Canada et ailleurs dans le monde.

À l'origine, Google a affirmé n'avoir pas recueilli de renseignements personnels.

Toutefois, en examinant les données détenues par l'entreprise, nos technologues ont découvert qu'elle avait bel et bien recueilli des renseignements personnels, dont certains étaient très sensibles. Tout indique que des milliers de Canadiens ont été touchés par cet incident.

Nous avons recommandé à Google de prendre des mesures pour s'assurer du respect des procédures nécessaires en matière de protection de la vie privée avant de lancer des produits et pour renforcer la formation donnée à ses employés à cet égard. Google a donné suite à nos préoccupations en mettant en œuvre plusieurs mesures correctives.

## Biométrie

La biométrie est une autre technologie naissante qui a également des ramifications importantes dans le domaine de la vie privée. Le terme « biométrie » désigne toute une gamme de techniques, de dispositifs et de systèmes utilisés par les appareils pour reconnaître les personnes ou confirmer leur identité en mesurant et en analysant des caractéristiques physiques et comportementales, entre autres les traits du visage, les empreintes digitales, les veines de la paume de la main, la signature vocale, la structure de l'œil et la démarche.

Les technologies biométriques, qui relevaient autrefois principalement du domaine de l'application de la loi, ont maintenant des applications dans le secteur commercial et dans l'administration publique en général. Toutefois, comme le Canada n'a adopté aucune politique sur l'utilisation de la biométrie, il n'existe aucune norme minimale régissant la protection de la vie privée, l'atténuation du risque ou la transparence envers le public.

En 2011, nous avons publié le document intitulé *Des données au bout des doigts*, qui explique les rudiments de la biométrie afin d'aider les Canadiens à comprendre ce domaine en rapide évolution. Ce document définit les risques que posent les technologies biométriques ainsi que les facteurs que devraient prendre en compte les organisations qui ont l'intention de les utiliser.

## Mesures de protection

Une protection adéquate des renseignements personnels est au cœur du droit à la vie privée. On ne s'étonnera donc pas que les mesures de protection aient occupé une place importante dans nombre de nos enquêtes et vérifications.

Par exemple, des vérifications réalisées en 2010 dans le secteur public ont révélé que l'utilisation d'appareils de communication portatifs et les pratiques d'élimination des ordinateurs excédentaires au sein de l'administration fédérale pouvaient porter atteinte à la sécurité des renseignements personnels des Canadiens.

En 2012, près de 6,5 millions de mots de passe cryptés ont été volés sur le site de réseautage LinkedIn et affichés en ligne.

Comme LinkedIn comptait alors de nombreux utilisateurs canadiens susceptibles d'être touchés par l'incident, le Commissariat a communiqué avec les responsables du site de réseautage pour examiner la portée de l'atteinte et évaluer son état de préparation et son intervention.

Nous avons constaté que LinkedIn avait immédiatement pris des mesures pour porter l'incident à l'attention de la haute direction, aviser les utilisateurs et cerner les causes de l'incident. Ces mesures et les autres interventions s'inscrivant dans la foulée de l'atteinte témoignent de la détermination de LinkedIn à prendre ses responsabilités.

Toutefois, nos discussions avec LinkedIn ont aussi mis en évidence certains aspects à améliorer concernant la gestion des mots de passe et l'accès au réseau. Les responsables ont répondu qu'ils mettraient en œuvre les mesures correctives voulues pour donner suite à nos préoccupations.

### **CE QUE CELA SIGNIFIE POUR VOUS**

Dans un monde de connectivité instantanée et de cyber-n'importe-quoi, la technologie est partout. Mais elle se trouve généralement en arrière-plan. Plus elle est omniprésente, moins nous la voyons.

Malheureusement, plus nous fermons les yeux sur la mécanique qui sous-tend ce miracle moderne, moins nous avons de chance de détecter ses lacunes. Et il devient de plus en plus difficile de protéger la vie privée.

Le travail accompli par le Commissariat dans le domaine de la technologie de l'information a contribué à déchiffrer certains aspects complexes. Nous avons relevé des cas de collecte ou de communication excessives de renseignements

personnels sans le consentement valable des intéressés. Nous avons mis au jour des problèmes de transparence et de sécurité de l'information.

La Direction de l'analyse des technologies et son laboratoire nous ont permis d'explorer les frontières de la technologie en acquérant des connaissances détaillées sur des technologies précises qui ont des répercussions sur la vie privée. Nous sommes maintenant en mesure de comprendre le langage technologique et de le parler avec les organisations du secteur privé et les institutions gouvernementales.

En consultant des spécialistes et en nous concentrant sur les nouvelles tendances d'avant-garde, nous avons également renforcé notre expertise interne et notre crédibilité auprès des intervenants. Nous avons ainsi pu donner des avis qui ont été bien accueillis et sensibiliser le public à toute une gamme d'enjeux importants.

### **PERSPECTIVES D'AVENIR**

En réalité, le rythme de plus en plus rapide des changements technologiques crée de nouveaux défis complexes et souvent imprévus dans le domaine de la vie privée.

Nous continuerons d'observer des cas mettant en jeu les technologies de l'information – et une utilisation de nouvelles technologies donnant lieu à la mise en œuvre d'initiatives qui ont des répercussions sur la vie privée en lien avec nos autres priorités stratégiques.

La difficulté sera de maintenir notre capacité interne à comprendre et à évaluer les répercussions sur la vie privée des nouvelles technologies de l'information en restant à l'avant-garde au lieu de perdre du terrain.



PRIORITÉ

# INTÉGRITÉ ET PROTECTION DE L'IDENTITÉ



## COMMENT TOUT A COMMENCÉ

La première fois que nous avons exploré cette priorité, nous songions au vol d'identité, lorsque des criminels s'emparent de renseignements personnels à des fins frauduleuses. Mais nous avons vite constaté que la question de l'intégrité et de la protection de l'identité est beaucoup plus large. En fait, toutes sortes d'entités s'approprient votre identité à longueur de journée, tous les jours – pour le meilleur ou pour le pire, et pour des raisons que nous pouvons ignorer ou ne pas comprendre ou encore avec lesquelles nous pouvons être en désaccord.

En cette ère de l'information, les gens laissent une trace lorsqu'ils naviguent en ligne, affichent un commentaire, utilisent une carte de crédit ou de fidélité, passent devant une caméra de surveillance, envoient un courriel au service à la clientèle d'une organisation ou effectuent tout autre type d'opération.

Vos éléments d'information sont recueillis, recoupés et analysés. Avec le logiciel d'analyse et le savoir-faire

voulus, les organisations peuvent établir votre profil de façon très détaillée – leur version de votre identité.

Elles peuvent utiliser cette identité à de multiples fins, par exemple pour obtenir un traitement de faveur dans un commerce ou vous inonder de publicité indésirable. Les gouvernements peuvent guetter les signes d'éventuels fauteurs de trouble. Si vos renseignements personnels tombent entre de mauvaises mains, vous pouvez devenir la proie d'escrocs. De nos jours, même des amateurs malintentionnés s'approprient l'identité d'autres personnes, ce qui donne lieu à des cas graves d'usurpation d'identité et de cyberintimidation.

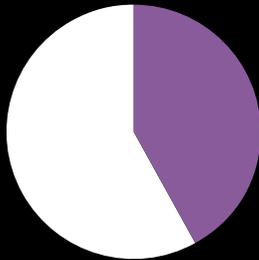
Le Commissariat s'efforce d'encourager les organisations des secteurs privé et public à améliorer leurs mesures de protection des renseignements personnels.

Nous encourageons également les gens à améliorer leurs connaissances numériques pour mieux gérer leur identité, particulièrement en ligne.

## LA VIE PRIVÉE EN CHIFFRES

Selon un sondage mené par le Commissariat, seulement 42 % des Canadiens estiment comprendre comment les nouvelles technologies peuvent porter atteinte à leur vie privée,

soit une baisse marquée par rapport à il y a une dizaine d'années.



**42 %**  
estiment  
comprendre

Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée, rapport final préparé pour le Commissariat à la protection de la vie privée du Canada par Phoenix SPI 2013.  
[http://www.priv.gc.ca/information/por-rop/2013/por\\_2013\\_01\\_f.asp](http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_f.asp)

Nous souhaitons que les gens comprennent ce qu'il peut advenir de leurs renseignements personnels dans le monde numérique et soient mieux outillés pour les maîtriser.

Tout cela revient à protéger l'intégrité de votre identité.

### CE QUE NOUS AVONS OBSERVÉ

Les travaux que nous avons menés en lien avec cette priorité stratégique ont révélé plusieurs tendances inquiétantes, en particulier la quantité phénoménale de renseignements numériques que les gens laissent derrière eux dans le quotidien, souvent à leur insu.

Par exemple, dans la rue, les allées et venues et les activités des gens sont systématiquement captées par des caméras de surveillance, les caméras utilisées pour créer les cartes Street View ou par d'autres citoyens qui se servent de la caméra de leur téléphone intelligent.

De nombreuses parties suivent les pages consultées par les internautes. Elles utilisent les renseignements personnels ainsi recueillis pour établir ou compléter le profil des internautes et leur acheminer des publicités ciblées ou s'en servent à d'autres fins dont ils ignorent tout.

Consciemment ou non, les gens divulguent des bribes de leur personnalité. En affichant des commentaires ou des photos en ligne, en utilisant des cartes de fidélité ou en communiquant leur emplacement au moyen d'un appareil doté de la fonction GPS, ils génèrent davantage de données d'intérêt pour certains.

En outre, les gens affichent de l'information concernant d'autres personnes. Il peut s'agir d'une jolie photo d'un ami ou de remarques désobligeantes concernant un « ennemi ». La cyberintimidation – et

ses conséquences potentiellement dévastatrices – posent désormais un problème grave dans les écoles à la grandeur du pays.

Cette tendance à afficher les renseignements personnels d'autres individus présente un défi hors du commun pour le Commissariat. En effet, de par sa conception, notre législation régit les pratiques des entités commerciales et de l'administration fédérale – et non celles des individus – dans le domaine de la protection de la vie privée.

### **CE QUE NOUS AVONS ACCOMPLI**

Compte tenu de l'évolution rapide des enjeux se rapportant à l'intégrité de l'identité, nous avons jugé important d'examiner la situation en détail et de solliciter l'avis de divers spécialistes du domaine.

Nos travaux sur ce front nous ont aidés à reconnaître et à mieux comprendre les nombreuses façons dont notre identité est façonnée et gérée, ce qui nous a permis de donner des avis et des conseils efficaces aux secteurs privé et public sur toute une gamme d'enjeux, notamment les initiatives gouvernementales de gestion de l'identité en ligne et la publicité comportementale en ligne.

En outre, nous avons aidé les gens à se prendre en main dans le domaine en créant des outils pour perfectionner leurs connaissances numériques.

Voici quelques exemples de nos activités.

## **Consultations sur la protection de la vie privée des consommateurs**

Dans le contexte numérique en pleine évolution, nous avons pris conscience du fait que les

Canadiens voulaient pouvoir adopter les nouvelles technologies et la cyberéconomie en toute quiétude sans renoncer à la pleine maîtrise de leurs renseignements personnels. C'est pourquoi nous avons mené en 2010 des consultations sur la vie privée des consommateurs pour mieux comprendre l'environnement en évolution et explorer les meilleures façons de protéger la vie privée dans le domaine au cours des années à venir.

Nous nous sommes concentrés, d'une part, sur le suivi, le profilage et le ciblage en ligne des consommateurs et, d'autre part, sur l'infonuagique, qui est décrite dans la section du présent document consacrée à la technologie de l'information.

Nous souhaitions en savoir plus sur certaines pratiques de l'industrie, explorer leurs répercussions sur la vie privée et connaître les attentes des Canadiens concernant les mesures de protection de la vie privée face à ces pratiques.

Des activités publiques webdiffusées, tenues à Toronto, à Montréal et à Calgary, ont permis de déterminer certains défis. Par exemple, certains participants ont déploré un manque de transparence entourant le suivi, le profilage et le ciblage en ligne, de sorte qu'il est pratiquement impossible d'obtenir le consentement valable requis en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) pour recueillir des renseignements personnels. Les inquiétudes exprimées par les participants à l'égard de la conservation permanente de renseignements en ligne ont incité le Commissariat à demander à l'industrie de régler ce problème en apportant des correctifs techniques.

## Le reste de l'iceberg

Nous ne présentons ici qu'une partie des activités menées par le Commissariat en lien avec la priorité stratégique Intégrité et protection de l'identité. On trouvera dans notre site Web une liste complète de nos activités, par exemple une description des enquêtes sur des problèmes d'intégrité de l'identité, des liens donnant accès à des outils qui permettent d'acquérir des connaissances numériques ainsi que des fiches d'information à l'intention des individus, notamment sur la réduction du risque de vol d'identité.

Des participants nous ont aussi fait part de préoccupations particulières à l'égard du suivi des enfants en ligne. Bien que leurs renseignements personnels soient particulièrement vulnérables, les enfants ne peuvent donner leur consentement à leur utilisation. Quel que soit leur âge, il faut protéger les enfants dans l'univers en ligne.

Les consultations nous ont permis d'obtenir une précieuse information sur les nouveaux défis qui surgissent dans la sphère numérique et sur des pistes de solution. Elles ont également préparé le terrain – et en fait créé un cadre – pour une grande partie de nos travaux portant sur l'intégrité et la protection de l'identité. Les consultations nous ont également aidés à nous forger une opinion sur la nécessité de mettre à jour la LPRPDE.

### Publicité comportementale en ligne

Les inquiétudes exprimées dans le cadre des consultations ont aidé le Commissariat à élaborer un énoncé de position et un document d'orientation sur la publicité comportementale en ligne.

Dans la publicité comportementale en ligne, un tiers que vous ne connaissez généralement pas suit votre navigation en ligne à votre insu et utilise l'information ainsi recueillie pour établir votre profil numérique. Les organisations se servent de votre profil pour connaître vos intérêts et vous transmettront des publicités en ligne ciblées ou d'autres messages destinés à vous inciter à faire des achats.

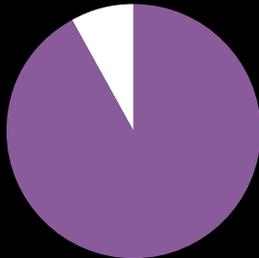
Nous estimons que l'information recueillie aux fins de la publicité comportementale en ligne constitue généralement des renseignements personnels selon la LPRPDE. Par conséquent, à notre avis, les individus doivent être dûment informés que leurs activités en ligne sont suivies et y consentir. Nous reconnaissons qu'un consentement négatif serait possible dans ce cas à condition de respecter certaines exigences et d'éviter certaines pratiques.

Dans notre *Position de principe sur la publicité comportementale en ligne* et nos lignes directrices intitulées *La protection de la vie privée et la publicité comportementale en ligne*, nous exhortons les organisations à éviter de suivre les enfants parce que ceux-ci ne peuvent donner un consentement valable. Nous demandons également que les individus

## LA VIE PRIVÉE EN CHIFFRES

Selon un sondage mené par le Commissariat, une forte majorité (73 %) de Canadiens comprennent que le gouvernement et des organisations commerciales peuvent suivre leurs activités en ligne. Moins de quatre répondants sur dix redoutent l'utilisation de cette information à des fins légitimes par le gouvernement ou les organismes d'application de la loi, mais la majorité estime que la surveillance générale exercée par l'État est une limite à ne pas dépasser. Près des trois quarts des répondants s'opposent à ce que les entreprises se servent de ces renseignements pour envoyer des pourriels.

Au dire d'une immense majorité (92 %), les entreprises devraient être tenues de demander l'autorisation de suivre les internautes en ligne.



92 %

Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée (2013)

disposent d'une façon raisonnable de détecter et de limiter cette pratique. Et nous faisons une mise en garde contre l'utilisation des pixels invisibles, des connexions malignes, des supertémoins, du piratage informatique, des empreintes d'appareil ou de toute nouvelle technique de suivi dissimulée que les utilisateurs ne peuvent voir.

## Littératie numérique

La nécessité d'intégrer la protection de la vie privée aux stratégies portant sur les connaissances numériques ou la citoyenneté numérique constitue un thème clé qui est ressorti des consultations sur la protection de la vie privée des consommateurs. Après tout, les menaces qui pèsent sur l'identité ne viennent pas simplement des autres. Les gens peuvent très facilement s'attirer des ennuis et en causer aux autres. Comme nombre de politiques et de célébrités l'ont découvert, il est vraiment plus facile de lancer dans le cyberspace une réflexion ou une image inappropriée que d'en reprendre possession.

Ces risques nous ont amenés à élaborer des fiches d'information et d'autres outils à l'intention des Canadiens de tous les groupes d'âge. Mentionnons notamment une fiche d'information générale sur la protection de la vie privée en ligne et d'autres fiches sur la publicité comportementale en ligne, l'utilisation des témoins et de l'infonuagique. Nous avons aussi élaboré des fiches de conseils concernant la protection des renseignements personnels sur les appareils mobiles pour une utilisation personnelle ou professionnelle.

Nous avons cherché des façons novatrices de sensibiliser les jeunes. Par exemple, nous avons produit une bande dessinée romanesque intitulée *Branchés et futés : Internet et vie privée* pour aider

les préadolescents et les jeunes adolescents à mieux comprendre les enjeux liés à la protection de la vie privée en lien avec le réseautage social, les appareils mobiles, la messagerie texte et le jeu en ligne et à s'y retrouver.

Nous avons aussi créé une trousse de présentation pour montrer aux élèves de différents niveaux quelle est l'incidence de la technologie sur leur vie privée et comment se construire une identité en ligne de manière sécuritaire et protéger ses renseignements personnels.

## Surveillance publique

Si vous vous promenez dans la rue de n'importe quelle ville ou dans un grand magasin, il y a de fortes chances que votre image soit captée par vidéosurveillance. L'utilisation des caméras est maintenant très répandue afin de limiter les infractions au code de la route, d'améliorer la sécurité des bâtiments et de faciliter l'application de la loi et pour une foule d'autres finalités.

En outre, les citoyens qui ont sur eux une caméra peuvent souvent prendre et partager des images de gens dans des lieux publics, en particulier lorsque survient un événement susceptible de faire les manchettes. Si l'on ajoute les systèmes perfectionnés de reconnaissance faciale et de reconnaissance des formes, les individus et les groupes sont de plus en plus sous surveillance.

Toutefois, à notre avis, le simple fait qu'une personne se trouve dans un lieu public ne l'oblige pas à renoncer à son droit à la vie privée.

En 2006, nous avons fait valoir cet argument dans les lignes directrices concernant le recours à la vidéosurveillance dans les lieux publics par les autorités chargées de l'application de la loi. En ce qui a trait au secteur privé, nous avons publié de nouvelles lignes directrices concernant la vidéosurveillance au moyen d'appareils non dissimulés en 2008 et la vidéosurveillance secrète en 2009.

En 2011, nous avons fait enquête sur une plainte déposée par une femme alléguant qu'une épicerie Sobeys avait recueilli ses renseignements personnels à son insu et sans son consentement au moyen de caméras vidéo. La plaignante alléguait également que l'entreprise lui avait refusé l'accès à ses renseignements personnels, y compris l'enregistrement de l'incident par vidéosurveillance. Nous avons conclu que Sobeys avait effectivement recueilli les renseignements personnels de la plaignante à son insu et sans son consentement étant donné que l'utilisation des caméras de surveillance n'était pas signalée de façon adéquate. Sobeys a accepté d'appliquer des autocollants sur la façade de ses magasins et d'installer un écran de surveillance en direct bien visible pour prévenir les clients de la surveillance.

Le Commissariat et trois commissariats provinciaux ont publié une fiche d'information sur l'imagerie à l'échelle de la rue. Nous avons indiqué que les entreprises devraient prendre des mesures pour mieux protéger la vie privée, par exemple utiliser des techniques de brouillage qui empêchent de voir les visages et les numéros de plaque d'immatriculation et mettre en place des mécanismes de réaction pour bloquer ou retirer les images lorsqu'il est possible d'identifier les personnes.



## Initiatives gouvernementales de gestion de l'identité

Le gouvernement fédéral continue de déployer un effort concerté pour adopter une démarche plus stratégique dans ses initiatives de gestion de l'identité. Depuis 2002, il s'est efforcé de créer des authentifiants communs plus économiques et sécuritaires pour donner accès aux services à l'échelle du gouvernement.

L'administration fédérale a récemment mis en œuvre la CléGC, service d'authentification grâce auquel les individus peuvent avoir accès aux programmes et services gouvernementaux en ligne en entrant un nom d'utilisateur et un mot de passe, et SecureKey Service de Concierge, service d'authentification grâce auquel ils y ont accès en entrant le nom d'utilisateur et le mot de passe qu'ils emploient pour accéder aux services en ligne de leur institution bancaire. Ces deux initiatives s'inscrivent dans la foulée de l'*Initiative de renouvellement de l'authentification électronique* du Secrétariat du Conseil du Trésor.

Le Commissariat a été abondamment consulté pendant les étapes de planification des différents services d'authentification au cours des 10 dernières années et il a examiné près d'une quinzaine d'évaluations des facteurs relatifs à la vie privée à cet égard.

Grâce à l'expertise acquise en menant nos activités en lien avec la priorité stratégique de l'intégrité de l'identité, nous avons pu réagir d'une manière stratégique et uniforme.

En outre, nous avons été consultés et nous avons donné des conseils au cours de l'élaboration de la *Norme sur la protection de la vie privée et le Web analytique* et de l'évaluation connexe des facteurs

relatifs à la vie privée pour orienter les institutions gouvernementales quant au mode d'utilisation du Web analytique. Cette nouvelle norme du Secrétariat du Conseil du Trésor a donné suite à la majorité des recommandations formulées par le Commissariat, en particulier en ce qui a trait à l'interdiction explicite d'utiliser l'information recueillie sur l'utilisation du Web pour établir le profil d'individus et aux délais prévus pour la conservation et l'élimination des renseignements personnels.

### CE QUE CELA SIGNIFIE POUR VOUS

Les efforts énergiques que nous avons déployés sur différents fronts en lien avec la priorité stratégique Intégrité et protection de l'identité – tant dans le secteur public que privé – nous ont aidés à bien connaître les défis et les risques auxquels font face les Canadiens.

Ils nous ont par ailleurs permis de collaborer avec des organisations et des individus pour trouver des solutions.

Par exemple, il nous est apparu évident que les technologies et modèles fonctionnels nouveaux vont à l'encontre des principes relatifs à l'équité dans le traitement de l'information.

À la fois dans les secteurs privé et public, nous constatons que des organisations recueillent de plus en plus de renseignements personnels qui doivent tous être protégés de façon adéquate.

Le secteur privé utilise l'analytique des données pour le suivi, le profilage et le ciblage des clients à la fois en ligne et hors ligne. L'administration fédérale se sert aussi des mêmes puissants outils d'analyse pour en savoir plus sur les Canadiens et répondre aux besoins urgents de la population. En outre, nous voyons un

nombre croissant de partenariats public-privé qui donnent lieu au partage de renseignements personnels.

Dans le secteur privé, en vertu de l'un des principes relatifs à l'équité dans le traitement de l'information à la base de la LPRPDE, les organisations doivent obtenir un consentement valable pour recueillir et utiliser des renseignements personnels. Ce n'est pas une tâche facile sur un ordinateur de bureau; alors, imaginez ce qu'il en est dans l'espace mobile avec un écran minuscule et l'attention de courte durée des utilisateurs.

Et le problème est aggravé par le fait que les gens se précipitent vers ces technologies, adoptent des applications de toutes sortes et affichent des renseignements sur eux-mêmes et sur d'autres personnes – même s'ils ne comprennent pas les conséquences de leurs actes sur la vie privée. Mais les gens sont autonomes et leurs activités, dans l'ensemble, ne relèvent pas de la législation sur la protection des renseignements personnels.

Nous nous sommes attachés à sensibiliser la population aux enjeux liés à la protection de la vie privée en lien avec l'intégrité de l'identité. Nous avons utilisé à cette fin divers moyens attrayants et stimulants – médias sociaux, multimédia, séries de conférences et bandes dessinées romanesques pour les jeunes.

Mais, bien entendu, il n'incombe pas uniquement aux individus de se protéger. Et c'est pourquoi nous avons élaboré des documents d'orientation, des outils et des initiatives de sensibilisation pour aider le gouvernement et les organisations du secteur privé à respecter leurs obligations en matière de protection de la vie privée. Nous avons également rencontré les représentants d'organisations et de ministères pour en savoir plus sur leurs pratiques actuelles et

nouvelles et leur faire part de nos commentaires sur les mesures à prendre afin de mieux protéger les renseignements personnels des Canadiens.

Nous sommes conscients que le gouvernement et le secteur privé sont toujours à l'affût de façons novatrices de communiquer avec les citoyens, les clients et les intervenants. Nous ne voulons pas freiner cet élan. Mais nous rappelons aux organisations que l'innovation repose sur la confiance des utilisateurs, elle-même fondée sur le respect de l'intégrité de l'identité des individus.

### **PERSPECTIVES D'AVENIR**

À mesure que les Canadiens continueront d'adopter des technologies nouvelles et plus intelligentes, les risques d'atteinte à la sécurité de leurs renseignements personnels et à l'intégrité de leur identité ne feront qu'augmenter.

L'idée selon laquelle « les gens ne se soucient pas de la protection de leur vie privée » est tout simplement erronée. La difficulté réside dans la communication de l'information et des idées concernant un sujet de plus en plus complexe d'une façon accessible et facile à comprendre.

Entre-temps, les organisations doivent s'assurer d'investir adéquatement dans la protection de la vie privée et d'intégrer les mesures de protection à leurs produits et services – dès le début.

Enfin, à notre avis, il faut renforcer la LPRPDE pour s'assurer que le droit des Canadiens à la vie privée est protégé comme il se doit en cette ère numérique et que leur identité et la façon dont ils choisissent de se présenter au reste du monde sont fondamentalement respectées.



# RENSEIGNEMENTS GÉNÉTIQUES ET PROTECTION DE LA VIE PRIVÉE

## COMMENT TOUT A COMMENCÉ

Lorsqu'il est question de renseignements personnels, rien n'est plus « personnel » que l'ADN d'un individu.

Il est vrai que notre bagage génétique est similaire à 99 %, mais le 1 % qui nous distingue fait de notre ADN l'identificateur suprême.

Qui plus est, notre information génétique ne constitue pas simplement une fiche d'information à notre sujet. Il s'agit d'une véritable bibliothèque. Elle relate l'histoire de nos ancêtres, de notre présent, voire de notre avenir.

Tout cela rend nos renseignements génétiques extraordinairement précieux à nos yeux – et extrêmement alléchants pour bien d'autres, les services de police, les chercheurs en médecine, les assureurs et notre patron.

Si le Commissariat a décidé de faire des renseignements génétiques l'une de ses priorités, ce n'est pas parce qu'il était inondé de plaintes ou de demandes de renseignements à cet égard. Pas du tout.

Mais nous nous inquiétons de l'incidence éventuelle sur la vie privée compte tenu de la progression rapide de la génétique.

Et nos inquiétudes initiales se sont confirmées dès que nous avons commencé à nous pencher sur cet aspect. Les risques d'atteinte à la vie privée sont déjà multiples, variés et d'une vaste portée. De surcroît, les technologies permettant de mettre ces renseignements sensibles entre les mains d'individus et d'organisations deviennent très accessibles.

Nous estimions que la génétique changerait la donne dans le domaine de la vie privée et nous avons

Selon un sondage mené par le Commissariat, si leur médecin leur recommandait de subir des tests génétiques, plus de la moitié des Canadiens craindraient

qu'on leur demande d'en communiquer les résultats à des fins non médicales, par exemple pour obtenir de l'assurance ou dans le cadre d'une demande d'emploi.

Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée (2013)

constaté – avec une certaine consternation – que nos craintes étaient plus fondées que nous le prévoyions.

### CE QUE NOUS AVONS OBSERVÉ

Depuis que nous avons défini les renseignements stratégiques comme une priorité, nous avons observé plusieurs tendances importantes.

L'utilisation des renseignements génétiques pour toute une gamme de tests qui ne servent pas à prévoir l'état de santé a monté en flèche au cours des dernières années.

Des tests relativement bon marché sont déjà offerts pour déterminer la paternité ou répondre à des questions concernant l'ascendance d'un individu. Des parents ont recours aux tests génétiques dans l'espoir de trouver des indices sur la probabilité que leur enfant devienne un athlète ou un musicien exceptionnel. Des gens paient aussi des entreprises proposant des tests de génomique nutritionnelle qui sont censés déterminer les types d'aliments qui conviennent le mieux à leur constitution génétique.

Tout cela signifie aussi qu'une quantité sans cesse croissante de renseignements génétiques aboutit entre les mains d'un nombre croissant d'entreprises privées – grandes et petites, de bonne réputation ou sans scrupules.

Des employeurs et des compagnies d'assurances voient aussi dans les renseignements génétiques un outil servant à déterminer qui risque davantage de tomber malade – et d'imposer ainsi un fardeau financier aux entreprises.

Entre-temps, les organismes chargés de l'application de la loi tirent de plus en plus parti des possibilités qu'offrent les tests génétiques.

Les services de police, les responsables de l'immigration et d'autres intervenants ont aussi testé des appareils portatifs permettant d'analyser rapidement l'ADN sur le terrain aux fins d'identification.

Ce tout nouvel outil d'analyse de l'ADN – Rapid DNA – est un autre exemple de l'interaction des avancées en génétique, d'une part, et du pouvoir croissant des technologies de l'information et de leurs coûts à la baisse, d'autre part.

Les avancées technologiques remettent par ailleurs en question l'hypothèse selon laquelle on peut facilement dépersonnaliser les renseignements génétiques, ce qui permettrait de les utiliser en recherche de façon anonyme.

Des chercheurs de l'Université Harvard ont récemment prouvé qu'ils avaient pu identifier plus de 40 % d'un échantillon de participants anonymes prenant part à une vaste étude de l'ADN menée par l'établissement.

### **CE QUE NOUS AVONS ACCOMPLI**

Dès 1995, alors que les tests génétiques en étaient encore à leurs balbutiements, le Commissariat a publié le rapport intitulé *Le dépistage génétique et la vie privée*. Le principal défi dont faisait état ce rapport était la nécessité de déterminer comment la société pourrait bénéficier des avantages qu'offre la génétique sans que celle-ci n'empiète sur l'autonomie et la perception de soi-même des individus.

Les avancées réalisées au fil des années qui ont suivi – le séquençage du génome humain et les progrès formidables en génétique – ont intensifié l'urgence de ce défi.

Grâce aux travaux que nous avons menés en lien avec la priorité stratégique des renseignements génétiques, nous sommes beaucoup mieux placés pour relever le défi.

En mettant sur pied un groupe de travail sur la confidentialité des renseignements génétiques, nous avons pu définir des priorités, construire une capacité interne et acquérir des connaissances.

Par exemple, dans le cadre d'un atelier que nous avons organisé en 2009 et auquel participaient des employés et plusieurs spécialistes de l'extérieur, nous avons discuté de quatre sujets, soit les biobanques, l'utilisation de l'ADN aux fins d'application de la loi, les tests génétiques offerts directement aux consommateurs et la discrimination génétique. Grâce à l'atelier, le personnel a grandement amélioré ses connaissances et son expertise, ce qui nous a permis de participer et de contribuer de façon plus pertinente au débat sur les politiques concernant la gouvernance et l'utilisation des renseignements génétiques, tout en nous aidant à définir nos priorités.

En outre, les relations de travail importantes que nous avons établies avec des centres d'expertise, comme Génome Canada, et plusieurs spécialistes universitaires nous ont permis de tirer parti de connaissances spécialisées. Nous avons participé à une série d'activités portant sur la génomique, la politique publique et la société, où nous avons abordé divers sujets – la génétique, le consentement et les biobanques; les renseignements génétiques et les assurances; et les tests génétiques offerts aux consommateurs en ligne.

Toutes ces activités ont renforcé notre capacité à appuyer et à éclairer le travail des décideurs et des parlementaires dans plusieurs dossiers, en particulier l'utilisation de l'ADN par les organismes chargés de l'application de la loi.

En outre, grâce à nos connaissances, nous avons été en mesure d'élaborer des produits d'information à l'intention du grand public.

Voici quelques exemples de nos activités.

## Tests génétiques

En 2010, le Commissariat a financé une étude qui portait sur les politiques de confidentialité des entreprises offrant un large éventail de tests génétiques directement aux consommateurs.

Cette étude propose à l'intention des Canadiens une liste de vérification de trois pages renfermant des questions sur la confidentialité à poser avant de faire affaire avec une entreprise qui offre des tests directement aux consommateurs.

Les consommateurs qui cherchent des réponses à leurs questions – en examinant attentivement la politique de confidentialité des entreprises et en communiquant directement avec ces dernières – pourront faire un choix plus éclairé quant à la pertinence d'envoyer leurs renseignements personnels et leurs échantillons génétiques à une entreprise.

Le Commissariat s'est associé avec Genome Canada pour organiser une série d'ateliers visant à favoriser le dialogue entre les décideurs et les chercheurs sur trois sujets : les tests offerts directement aux consommateurs, la discrimination génétique et le rôle du consentement dans la recherche faisant appel aux biobanques. À l'issue des ateliers, on a publié des mémoires de politique visant à éclairer le débat et la discussion sur ces trois sujets.

## Génétique et assurances

L'utilisation éventuelle des renseignements génétiques par les compagnies d'assurances constitue un autre aspect de la confidentialité de ces renseignements qui évolue rapidement.

Contrairement à la situation observée dans d'autres pays, par exemple aux États-Unis, il n'y a aucune loi au Canada qui régit expressément l'utilisation des renseignements génétiques par les compagnies d'assurances. En outre, aucun gouvernement n'a imposé un moratoire sur l'utilisation de ces renseignements à des fins d'assurances comme c'est le cas dans certains pays d'Europe.

Selon la position adoptée par l'Association canadienne des compagnies d'assurances de personnes, même si les assureurs n'exigent pas qu'un proposant subisse des tests génétiques, un assureur peut demander l'accès aux résultats si un proposant en a subi.

Pour nous aider à mieux comprendre l'industrie et évaluer la position de l'Association, le Commissariat a demandé à deux spécialistes universitaires d'analyser l'argument de l'industrie selon lequel les assureurs doivent avoir accès aux renseignements génétiques pour évaluer les risques de façon exacte et équitable.

Les spécialistes ont conclu que l'interdiction d'utiliser les renseignements génétiques n'aurait pas de répercussions négatives importantes à l'heure actuelle et à court terme sur les assureurs ou sur la viabilité du marché de l'assurance.

En guise de suivi, nous avons organisé une table ronde avec divers intervenants.

La table ronde et la recherche que nous avons commandée nous aideront à déterminer si les assureurs ont besoin de recueillir et d'utiliser ces renseignements et si une personne raisonnable considérerait que leur collecte et leur utilisation sont appropriées dans les circonstances.

Pour mieux sensibiliser le public à la nature prédictive de la génétique, nous avons affiché dans notre site Web une série de questions et réponses en collaboration avec le professeur de médecine de l'Université de Toronto, le D<sup>r</sup> Steve Scherer, qui dirige le Centre de génomique appliquée à l'Hôpital pour enfants malades.

## Génétique et application de la loi

L'utilisation croissante des renseignements génétiques par les organismes d'application de la loi est un domaine où le Commissariat a été particulièrement actif au cours des dernières années.

Au Canada, la Banque nationale de données génétiques en 2000 visait à l'origine le catalogage de l'ADN prélevé sur les scènes de crime et de l'ADN de toute personne condamnée pour 37 infractions de nature violente ou sexuelle très graves. Toutefois, la liste de ces « infractions désignées » a été allongée et elle compte maintenant plus de 265 infractions, ce qui accroît grandement le nombre de citoyens dont l'identificateur suprême est maintenant fiché dans les dossiers de la Gendarmerie royale du Canada.

À titre de membre d'office du comité consultatif de la Banque nationale de données génétiques,

le Commissariat participe à la surveillance de la banque.

Nous avons commandé une recherche pour comparer le cadre juridique qui régit l'établissement des banques de données génétiques à des fins d'enquête médico-légale au Canada avec celui du Royaume-Uni, de l'Australie, des Pays-Bas, du système fédéral américain et des États de la Californie, du Maryland et de New York. L'étude a révélé que les lois canadiennes régissant les banques de données imposent dans l'ensemble des restrictions égales ou supérieures par rapport aux règles en vigueur dans ces autres pays ou dans ces États.

En outre, le Commissariat a régulièrement commenté les enjeux liés à la protection de la vie privée se rapportant à l'utilisation de l'ADN à des fins d'enquête médico-légale dans des allocutions données à titre de membre du comité consultatif de la Banque nationale de données génétiques et dans des mémoires présentés dans le cadre d'examen systématiques de la législation habilitante effectués par le Parlement.

Il a été proposé d'élargir davantage l'utilisation de la Banque nationale de données génétiques en permettant les recherches « familiales ».

Par exemple, supposons que les services de police aient un échantillon d'ADN humain prélevé sur la scène d'un crime. Si une recherche dans la Banque nationale de données génétiques ne permet pas de trouver une concordance parfaite, les services de police pourraient chercher une quasi-concordance, car un parent proche est susceptible d'avoir un profil génétique similaire.

Dans la perspective du droit à la vie privée, les recherches familiales sont inquiétantes, car elles transforment les gens en suspects éventuels non pas en raison de ce qu'ils ont fait, mais simplement sur la base de leurs relations familiales.

Dans des allocutions publiques et des présentations devant des comités parlementaires, le Commissariat a fait valoir des arguments contre les recherches familiales pour des raisons juridiques, éthiques et opérationnelles.

De même, le Commissariat s'est opposé aux propositions préconisant que l'ADN de personnes soit stocké dans la Banque nationale de données génétiques dès leur arrestation.

Le prélèvement d'ADN dès l'arrestation revient à conserver des renseignements personnels extrêmement sensibles d'individus qui pourraient bien être des citoyens respectueux de la loi – même s'ils ont été arrêtés.

## Recherche en santé

Le Commissariat a examiné des évaluations des facteurs relatifs à la vie privée se rapportant à une étude longitudinale de Statistique Canada qui explore la relation entre, d'une part, les facteurs de risque de maladie et l'état de santé et, d'autre part, la mise au jour des problèmes de santé publique.

*L'Enquête canadienne sur les mesures de la santé* repose sur la collecte de milliers d'échantillons biologiques, y compris des échantillons d'ADN.

Nous avons formulé plusieurs recommandations pour mieux protéger la vie privée des participants

volontaires. Par exemple, nous avons exhorté Statistique Canada à fournir aux participants de l'information sur la recherche proposée à mesure qu'elle devient disponible afin de leur permettre de reconfirmer ou de retirer leur consentement à la lumière de cette nouvelle information. Nous avons aussi recommandé d'expliquer clairement aux participants ce qu'il advient de leurs échantillons s'ils retirent leur consentement.

Cet exemple met en évidence la nécessité de prendre en compte la protection de la vie privée lorsque l'on mène une recherche scientifique, aussi bénéfique soit-elle pour la société.

### **CE QUE CELA SIGNIFIE POUR VOUS**

Faire des renseignements génétiques l'une de nos priorités stratégiques, a donné au Commissariat la possibilité d'acquérir des connaissances et d'adopter une approche prospective. Cette expérience d'apprentissage nous a permis de cerner les futurs enjeux liés à la protection de la vie privée qui auront une très grande incidence sur la vie des Canadiens et de commencer à nous y préparer.

Nous sommes maintenant beaucoup mieux placés pour évaluer les conséquences sur la vie privée et les répercussions au chapitre des principes relatifs à l'équité dans le traitement de l'information à la base de la législation canadienne sur la protection de la vie privée.

En outre, nous sommes parvenus à comprendre le contexte international des initiatives législatives visant à protéger les renseignements génétiques. Nous entretenons par ailleurs des relations avec des universitaires, le gouvernement, l'industrie de l'assurance et d'autres intervenants pour nous

assurer de rester au fait des changements rapides qui surviennent.

Tous ces efforts nous ont permis de formuler des avis plus éclairés à l'intention des parlementaires et des décideurs fédéraux. Nous avons pu mettre en évidence les préoccupations en matière de vie privée dans le domaine de la génétique.

Nous estimons que toutes nos activités en lien avec cette priorité seront utiles dans nos discussions stratégiques et contribueront au vaste débat public continu sur les renseignements génétiques et la protection de la vie privée.

#### **PERSPECTIVES D'AVENIR**

La génétique a déjà progressé à un rythme époustouflant et nous commençons à constater que les renseignements génétiques sont largement utilisés dans plusieurs contextes qui soulèvent des enjeux liés à la protection de la vie privée – par exemple les assurances, l'emploi et les tests génétiques directement offerts aux consommateurs.

De toute évidence, nous en sommes encore au début de l'utilisation des renseignements génétiques. Nous devons examiner minutieusement les répercussions éventuelles sur la vie privée pour élaborer des principes solides qui aideront à atténuer ces risques à l'avenir.





# LA VOIE À SUIVRE

Les quatre priorités retenues – la sécurité publique, la technologie de l'information, l'intégrité de l'identité et les renseignements génétiques – représentent les enjeux liés à la protection de la vie privée les plus urgents auxquels les Canadiens ont fait face au cours des dernières années.

Tout porte à croire que le paysage de la vie privée continuera d'évoluer rapidement et que des défis nouveaux et complexes nous attendent dans ces domaines.

## CONVERGENCE

En concentrant nos efforts, nous avons pu mettre en évidence certains points communs entre toutes les priorités qui continueront indubitablement de créer des défis sur le front de la vie privée au cours des années à venir.

Premièrement, la technologie de l'information constitue un élément déclencheur pour la grande majorité des défis naissants sur le front de la protection de la vie privée au cours de 21<sup>e</sup> siècle.

Les technologies peuvent engendrer des bienfaits considérables, mais la progression des technologies

et des techniques d'analyse continuera de présenter des défis indéniables sur le front des quatre priorités stratégiques.

En réalité, les risques d'atteinte à la vie privée découlant de certains enjeux se sont accrus au cours des dernières années à mesure que nous développons des technologies plus avancées et que le coût de la conservation de l'information et du déploiement de certaines technologies dégringolait.

À mesure que les utilisations réelles et potentielles de ces technologies apparaissent plus clairement, leur utilisation suscitait un intérêt accru tant dans le secteur public que privé.

Nous constatons de plus en plus que l'importance des renseignements personnels pour les entreprises et le gouvernement réside dans l'information qui est *dérivée* des données que nous fournissons comme consommateurs. Il s'agit d'un autre thème commun. C'est l'une des caractéristiques des mégadonnées.

Cette situation continuera de soulever des questions concernant l'approche traditionnelle de protection des données.

L'une des caractéristiques clés des mégadonnées est « davantage » – recueillir davantage et utiliser davantage. Mais cette pratique va à l'encontre des principales mesures de protection de la vie privée, en particulier le principe selon lequel on peut recueillir et utiliser les renseignements personnels uniquement à une fin particulière déterminée. Comment le consentement s'appliquera-t-il dans ce type d'environnement?

L'importance croissante accordée à l'utilisation des renseignements personnels à des fins prédictives – par exemple dans le cas de la publicité comportementale en ligne (Qu'est-ce que telle personne est susceptible d'acheter?), de l'application de la loi (Qui est un terroriste potentiel?) et des tests génétiques (Suis-je à risque de contracter une maladie en particulier?).

Dans la perspective de la vie privée, la capacité prédictive évoque la possibilité que des décisions nous concernant soient fondées sur des renseignements inexacts ou incomplets ou que des organisations puissent en savoir davantage que nous-mêmes à notre sujet.

### **COOPÉRATION INTERNATIONALE**

Dans les quatre domaines prioritaires, nous avons aussi constaté l'importance primordiale de la collaboration et de la coopération internationales.

Dans un monde numérique en réseau, les enjeux liés à la protection de la vie privée ont pris une envergure mondiale.

Partout sur la planète, les gens comptent sur les technologies de l'information et des communications communes – nous partageons de l'information, des

vidéos et des photos sur quelques plateformes de réseautage social très prisées, nous jouons en ligne sur les mêmes plateformes et nous utilisons les mêmes moteurs de recherche. Les individus achètent de plus en plus de biens et de services auprès d'organisations établies à l'étranger.

Compte tenu de ces tendances, lorsqu'une entreprise mondiale modifie ses pratiques de protection de la vie privée ou, pis encore, qu'elle est victime d'une atteinte à la sécurité des renseignements, des millions de gens dans le monde peuvent être touchés.

Entre-temps, la mondialisation a aussi eu une incidence considérable sur l'application de la loi et la sécurité publique – par exemple l'échange entre les pays des renseignements personnels concernant les voyages par avion et le contrôle frontalier.

Les enjeux mondiaux exigent une intervention d'envergure mondiale. C'est pourquoi le Commissariat s'efforce d'encourager la coopération en participant activement à plusieurs organisations internationales.

Mentionnons notamment l'Organisation de coopération et de développement économiques (OCDE), Coopération économique de la zone Asie-Pacifique (APEC), le Global Privacy Enforcement Network (GPEN), l'Association francophone des autorités de protection des données personnelles et l'Organisation internationale de normalisation (ISO).

### **LÉGISLATION MODERNE**

L'évolution rapide de chaque priorité a aussi mis en lumière la nécessité d'examiner et de mettre à jour les lois sur la protection de la vie privée pour les adapter aux nouvelles tendances.

Nos lois, nos politiques et nos institutions ont toutes été mises à rude épreuve au cours des 10 dernières années en raison de l'évolution rapide du monde commercial, de la préoccupation des gouvernements à l'égard de la sécurité et des attentes du public en constante évolution.

Selon de nombreux observateurs, cette situation remet en cause le cadre canadien de protection des renseignements personnels – dans les secteurs public et privé.

À notre avis, le moment est venu de moderniser la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* pour nous assurer qu'elles permettront de relever les défis d'aujourd'hui – et ceux qui nous attendent.

Les Canadiens méritent des lois modernes et pertinentes qui protègent leur vie privée et ils s'attendent à ce type de protection.

### UNE QUESTION D'ÉTHIQUE

Tous ces enjeux sont extrêmement importants pour l'avenir du Canada. Ils soulèvent non seulement des questions touchant le droit à la vie privée, mais aussi des questions morales et éthiques. Et ils ont des répercussions pour les générations futures.

Les Canadiens nous ont indiqué que le droit à la vie privée constitue une valeur qui leur est chère. Il s'agit d'une pierre angulaire de notre démocratie et d'un élément essentiel de toute société libre. Sans ce droit, aucune véritable liberté n'est possible.

C'est pourquoi il est primordial de faire des choix éclairés.

Les décisions que nous prenons aujourd'hui concernant les initiatives de sécurité publique, les technologies utilisées dans le quotidien et les politiques et les lois qui protègent nos renseignements personnels auront des conséquences pendant longtemps.

La question principale que les gouvernements, les organisations et les individus doivent se poser n'est plus seulement : « La loi de protection de la vie privée permet-elle cela? », mais plutôt « Devrions-nous faire cela? ».

Autrement dit, comment nous définissons-nous? Quelles relations entretenons-nous avec les autres, les organisations et les gouvernements? Essentiellement, *dans quel monde voulons-nous vivre?*

## Pour en savoir plus, contacter :

Téléphone : 1-800-282-1376  
Téléscripteur/ATS : 613-992-9190

[priv.gc.ca](http://priv.gc.ca)  
Suivez-nous sur Twitter : @PriveePrivacy



Commissariat  
à la protection de  
la vie privée du Canada