Rapport annuel
Commissaire à la
Protection de la vie privée
1998-99

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

(613) 995-2410, 1-800-267-0441
Téléc. (613) 947-6850
ATS (613) 992-9190

N° de cat. IP 30-1/1999
ISBN 0-662-64334-8

Cette publication est offerte sur cassette et sur disquette informatique.
Nous sommes accessibles sur le réseau Internet à : http://www.privcom.gc.ca

Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

juillet 1999

L'honorable Gildas L. Molgat
Président
Sénat
Ottawa

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1er avril 1998 au 31 mars 1999.

Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips

Bruce Phillips

Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

juillet 1999

L'honorable Gilbert Parent
Président
Chambre des communes
Ottawa

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1er avril 1998 au 31 mars 1999.

Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips

Bruce Phillips

Le saviez-vous ?

Vous ne craignez pas d'atteinte à votre vie privée ? Vous devriez peut-être vous raviser. Voici seulement quelques-unes des histoires que nous avons entendues l'an dernier.

- La société A.C. Neilson, spécialiste des études de marché, a breveté un système de reconnaissance des visages permettant d'identifier secrètement les consommateurs pour découvrir leurs habitudes d'achat.
- Deux épiceries ontariennes ont décidé de demander à des assistés sociaux d'apposer l'empreinte de leur pouce sur leurs chèques avant de les encaisser. La carte remise aux assistés sociaux de l'Ontario porte une telle empreinte, numérisée. Ces deux magasins ont cessé cette pratique après qu'un client s'est plaint auprès du commissaire ontarien à la protection de la vie privée.
- La police a capturé un groupe de la région de Toronto qui filmait secrètement des utilisateurs de cartes de débit en train de composer leur NIP, puis écoutait clandestinement les communications téléphoniques des magasins avant de se servir de cette information pour vider les comptes bancaires des clients.
- Des entreprises étudient de plus en plus votre alimentation, votre habillement, vous préférences télévisuelles, vos moyens de transport et vos divertissements, afin de découvrir les habitudes des consommateurs; par exemple, des spécialistes du marketing ont découvert que les hommes qui vont chercher des couches le soir sont plus susceptibles d'acheter de la bière avant de rentrer chez eux.
- Quelques sites Web enregistrent vos déplacements sur leurs pages et les renseignements que vous téléchargez; de plus, certains vous envoient des fichiers cachés ("cookies") qui les aident à vous reconnaître lors de vos visites subséquentes.
- Les employeurs peuvent maintenant déterminer les passe-temps, les intérêts et les valeurs des personnes qui postulent un emploi chez eux en examinant les sites Web qu'elles visitent. Selon une société de gestion de la sécurité de Calgary qui effectue des vérifications d'antécédents, une recherche sur les habitudes Web d'une personne peut en dire long sur celle-ci, en bien ou en mal.

- Le gouvernement du Québec envisage de créer une base centrale de données sur tous les Québécois, qui comporterait des noms, des photos et des renseignements signalétiques de base.
- Les visiteurs du site Web de la compagnie Nissan qui voulaient de l'information sur son nouveau véhicule Xterra ont obtenu beaucoup plus : les adresses électroniques de 24 000 autres acheteurs en puissance.
- Plusieurs magasins à succursales admettent qu'ils révèlent aux forces de l'ordre les habitudes d'achat de ceux de leurs clients qui détiennent leur carte de fidélité.
- Un échantillon d'urine ne permet pas de découvrir si quelqu'un est intoxiqué par une drogue, mais seulement si cette personne a utilisé cette drogue au cours des trente jours qui précèdent.
- Votre employeur peut lire votre courrier électronique, accéder à vos documents informatiques, surveiller les sites Internet que vous visitez et écouter votre courrier vocal.
- Si vous êtes l'un(e) des 7,2 millions de titulaires de cartes Air Miles, sachez que vos décisions d'achat sont communiquées aux 134 sociétés commanditaires chaque fois que vous utilisez votre carte. La compagnie Air Miles trie et groupe ces données pour ces sociétés. Tout ce qu'une succursale Blockbuster Video sait des préférences d'une personne en matière de films, le magasin des alcools de votre région peut le savoir également, et vice versa.
- Les renseignements personnels de centaines de titulaires de cartes Air Miles (numéro de carte, nom, numéro de téléphone personnel, adresse électronique, nom de l'employeur et numéro de téléphone au travail) ont été accessibles par Internet pendant plusieurs mois, et peut-être même pendant près d'un an.
- Il paraît que la *Michigan Commission on Genetic Privacy* propose que l'état conserve en permanence les échantillons de sang qu'il obtient des nouveau-nés pour dépister les maladies congénitales rares. La Commission croit en effet que ces échantillons pourraient constitue une ressource précieuse pour les forces de l'ordre et les chercheurs scientifiques.

- Le fait de dissocier le nom d'une personne de ses renseignements personnels et de combiner ces derniers avec des données sur d'autres personnes ne garantit pas la protection de cette information. Il existe enfin des techniques permettant aux chercheurs d'identifier un individu à partir de statistiques agrégées en associant celles-ci à de l'information publique. Par exemple, si l'on sait que cinq pour cent des gens faisant partie d'un groupe de 20 personnes ont plus de 65 ans et gagnent plus de 100 000 $, il est possible de trouver madame Unetelle, âgée de 67 ans, dans les archives publiques et d'en deviner le revenu.
- Plusieurs entreprises britanniques consultent des scientifiques au sujet de la possibilité d'implanter une puce informatique dans leurs employés pour surveiller leurs allées et venues et leur horaire. Un scientifique a mis au point une telle puce, qu'il s'est même fait implanter pour prouver son efficacité.
- Le fournisseur d'accès Internet America Online reçoit régulièrement des ordonnances de tribunaux pour l'obtention de renseignements sur des abonnés impliqués dans un divorce ou dans un litige portant sur la garde d'enfants.

Nous tenons à remercier Chris Slane, caricaturiste professionnel et fils de Bruce Slane, commissaire néo-zélandais à la protection de la vie privée, de nous avoir autorisé à reproduire des caricatures extraites de sa plus récente collection, intitulée *Let me through, I have a morbid curiosity*.

Table des matières

L'ère de la résignation ?

Nous n'ouvrons le débat ni avec des cris ni des larmes. Posons plutôt certaines questions :

Vaut-il la peine de préserver la vie privée ?

Le début du nouveau millénaire sonnera-t-il la fin du droit à la vie privée ?

Sommes-nous à l'aube de l'ère de la résignation ?

Ces questions, nous ne les posons pas par pure forme ou en théorie. De plus en plus de milieux les soulèvent et cherchent à y répondre. Au moment de mettre sous presse, nous avons constaté une avalanche de publications connues traitant du sujet. On pourrait résumer ainsi leurs terribles conclusions : la technologie a gagné, les droits de la personne ont perdu, la vie privée n'existe plus, donc aussi bien s'y faire.

La synthèse la plus incisive de ce point de vue est parue le 1er mai dans le très respecté périodique *The Economist*. Signalant que la société faisait déjà l'objet d'une omniprésente surveillance (une situation maintes fois soulignée dans nos rapports annuels), *The Economist* avance qu'il est utopique d'essayer de retrouver la vie privée dont nous jouissions dans les années 1970.

Selon l'article, "la technologie informatique évolue tellement vite qu'il est difficile de prédire comment elle sera appliquée. Mais certaines tendances ne trompent pas. Le volume de données consigné sur les gens continuera d'augmenter de façon très marquée. Les conflits sur la vie privée s'envenimeront. Les tentatives pour freiner la société de surveillance à coup de lois s'intensifieront [...] Mais voici une audacieuse prédiction : tous ces efforts pour empêcher la vague montante de l'intrusion électronique dans la vie privée seront vains. Les gens devront commencer à accepter qu'ils n'ont tout simplement plus de vie privée. Ce sera là l'un des plus grands changements sociaux des temps modernes." [traduction]

L'article déduit que certaines personnes choisiraient même, si elles le pouvaient, de renoncer aux énormes avantages qu'offre (soi-disant) une économie de l'information (des rues plus sûres, des communications plus abordables, plus de divertissements, de meilleurs services gouvernementaux). Mais ces personnes ne se verront jamais offrir un tel choix et la perte cumulative de leur contrôle sur leurs renseignements personnels signifiera la fin de la vie privée.

Presque simultanément, le politicologue Reg Whitaker, de l'Université York, a publié son livre *The End of Privacy: How Total Surveillance is Becoming a Reality*. M. Whitaker rappelle le concept de la prison panoptique proposée par Jeremy Bentham au XVIIIe siècle (décrite dans notre rapport annuel de 1996-1997). Il s'agissait d'une prison dotée d'une tour centrale de laquelle les gardiens pourraient observer les détenus autour du périmètre sans en être vus. La tour pouvait bien être inoccupée mais sa simple présence assurait le fonctionnement automatique du pouvoir.

M. Whitaker prétend que les nouvelles peuvent mener à une omniscience des plus réelles. L'inspecteur panoptique centralisé de Jeremy Bentham se verrait remplacer par une multitude d'inspecteurs tout aussi panoptiques, mais décentralisés. Chaque fois que nous effectuons une transaction qui est enregistrée (comme le sont désormais toutes les transactions), nos données clignotent sur le réseau. Selon Whitaker, cette transparence momentanée cède la place à une image précise lorsqu'elle est rajoutée à toutes ces autres transactions que nous effectuons.

Mais notre prison panoptique actuelle est encore mieux que l'ancien modèle : en effet, nous y participons volontairement, car nous choisissons de n'en voir que le côté pratique, rapide et sécuritaire. Nous refusons d'en considérer les désavantages, dont le pire est la conformité que provoque la crainte de se savoir surveillé à chaque instant. N'ayons pas peur des mots : notre liberté en est diminuée d'autant, quand elle ne disparaît pas complètement.

Bienvenue au débat!

Ces arguments ne sont peut-être pas nouveaux, mais le fait qu'ils reviennent de plus en plus souvent démontre clairement notre prise croissante de conscience des profondes répercussions que notre utilisation insouciante de la technologie de surveillance a sur notre société. Voici ce que je réponds à *The Economist* et à Reg Whitaker : je ne conteste pas votre prédiction, mais je ne crois pas en son inéluctabilité. Nous avons encore beaucoup de notre vie privée à perdre. C'est donc avec plaisir que je vous accueille dans le débat, car il est temps de s'attaquer sérieusement à ce sujet.

Les tenants d'une vie privée se voient souvent accusés de s'opposer à une société "ouverte", comme si la liberté d'expression et de presse obligeait tout le monde à vivre dans un "aquarium". Il est clair que les gouvernements doivent rendre des comptes aux citoyens afin de permettre à ces derniers de

juger de la qualité de leurs politiques et de leur gestion. Et les médias ont le droit (et le devoir) de soulever les enjeux d'intérêt public d'une façon que nous espérons exacte et juste. Mais les citoyens d'une société libre ne sont nullement obligés de déballer toute leur vie à leurs gouvernements, leurs voisins ou aux médias. Bien que certains programmes télévisés prouvent que certains citoyens peuvent choisir de dévoiler plus de détails personnels que nous ne le souhaiterions, il n'en reste pas moins que chacun d'entre nous est seul responsable de décider de ces détails et à qui nous les communiquons. Le respect de la bulle de notre prochain est une des caractéristiques d'une société libre.

Ne vous inquiétez pas, Mme Davidson : c'est une simple puce informatique derrière l'oreille. Les consciences tranquilles n'ont rien à craindre.

Ceux qui clament la culpabilité automatique de toute personne "ayant quelque chose à cacher" ne font que perpétuer le mythe voulant que la notion de vie privée ne serve qu'à dissimuler des secrets inavouables. En fait,

il n'y a qu'à poser les bonnes questions à n'importe quel mordu des nouvelles technologies : tôt ou tard, il refusera de vous répondre, peut-être sur le sujet de ses finances, de ses préférences sexuelles ou de son état de santé. Chacun d'entre nous "a quelque chose à cacher", et nous avons le droit de le cacher car cela ne concerne personne d'autre (à part peut-être certains proches). Ceux d'entre nous qui ont eu le malheur de connaître un régime politique ne respectant nullement la vie privée de sa population savent à quel point une telle ingérence gouvernementale mène à un contrôle social et à un affaiblissement des volontés individuelles.

Accorder la priorité aux valeurs humaines

D'autres encore prétendent que les défenseurs du droit à la vie privée sont tous des Luddites ou des technophobes qui s'opposent aux nouvelles technologies. Ces gens présument que nous refusons ces nouveaux outils, et leur attitude porte à croire que de telles technologies doivent obligatoirement voir le jour. Rien n'est plus faux. Non seulement nous utilisons ces nouvelles technologies, mais nous les apprécions : leur attirance est grande car elles sont libératrices et puissantes. Mais nous en voyons aussi les désavantages. Ce sont des valeurs humaines, et non technologiques, qui doivent piloter notre vie. Si nous le voulons réellement, nous pouvons incorporer aux nouvelles technologies des composantes qui protégeront notre vie privée et la confidentialité de nos renseignements personnels. À en croire son plus haut responsable en matière d'informatique, le gouvernement fédéral semble prêt à le faire. En effet, le gouvernement vient d'adopter le principe fondamental voulant que la protection de la vie privée ne soit pas un obstacle, mais bien une composante essentielle de tout projet informatique. Une décision encourageante.

Je pense qu'à la longue, les fatalistes auront tort. La situation pourrait empirer passablement avant de s'améliorer, ce qu'elle fera si le public persiste dans son indifférence et son ignorance. La rapidité et l'étendue des changements sont tout aussi phénoménales que la réaction de la société face à ces derniers. Mon mandat n'est pas encore révolu que les médias sont déjà passés d'un rejet initial de nos mises en garde comme étant exagérées et alarmistes à un abject abandon de la lutte.

Le véritable problème n'est pas la technologie ni certaines de ses séduisantes promesses de facilité, de sécurité et d'efficience. C'est en fait notre incompréhension des énormes coûts qui sont le lot de l'insinuation effrénée de la technologie dans chacun des aspects de notre vie moderne.

Notre âme en échange de points?
Nos multiples tracas quotidiens rendent freinent notre sensibilité aux courants profonds qui viennent bouleverser la société. Il est beaucoup plus facile de comprendre la valeur concrète immédiate du rabais que procure une carte de fidélité que les répercussions à long terme de la collecte sans cesse croissante de renseignements personnels. Mais chaque divulgation en apparence anodine de ces renseignements finit par offrir les moindres détails de notre vie en pâture à toutes les grandes entreprises et les institutions gouvernementales. Nous aurons fini par vendre notre âme en échange de quelques points d'un club quelconque de fidélité.

Le véritable danger qui guette notre vie privée n'aura donc jamais été la perspective d'un quelconque cataclysme qui nous ferait monter aux barricades. C'est plutôt la disparition progressive de notre contrôle sur nos renseignements personnels, ainsi que notre acceptation passive ou inconsciente des conséquences à long terme. L'histoire nous a pourtant souvent appris que c'est par petites doses que la liberté finit par mourir.

La fin de la vie privée telle que le conçoit *The Economist* (dont les arguments ont hélas été trop souvent et trop avidement acceptés par des légions de bureaucrates et de cadres d'entreprises) se réduisent à ceci : nous échangerons sans hésiter notre liberté contre la séduisante perspective de jouir d'une plus grande sécurité, d'une plus grande efficience et d'une plus grande facilité. Selon M. Whitaker, "Big Brother" ne nous surveille plus : il nous protège. La technologie gérée par l'état et l'entreprise privée deviendra notre maîtresse, et nous deviendrons ses esclaves. Nous sommes en fait en train de nous préparer un Goulag électronique.

Peut-être n'y a-t-il pas suffisamment de gens qui savent que les notions de vie privée et de liberté sont inextricablement liées : l'une ne saurait exister sans l'autre. Ceux qui en doutent devraient réfléchir à ceci : pour évaluer le degré de liberté dont jouit une société, commencez par évaluer le niveau de vie privée dont jouissent ses habitants. Le lien est frappant. C'est ce qui explique l'extrême préoccupation de certains pays européens telle l'Allemagne laquelle, consciente des erreurs de son passé, est désormais à l'avant-garde en matière de protection des renseignements personnels.

Mais cette méconnaissance du lien entre les deux notions précédentes est répandue, et donne naissance à une foule de notions douteuses. Ainsi, un chroniqueur bien en vue a récemment postulé qu'une carte d'identité

nationale obligatoire serait l'unique solution à la lutte contre la fraude dans les domaines de l'immigration, du bien-être social et de l'assurance santé.

Des murs de papier

Négligeant le fait bien prouvé que les escrocs trouveront toujours un moyen de déjouer le système, cette suggestion bafoue complètement les droits fondamentaux, et revient à dire qu'il vaut mieux contrôler toute une population dans l'espoir d'attraper quelques fraudeurs. En fait, pour être plus précis, cela revient à dire qu'il est plus facile de surveiller chaque citoyen que de contraindre les bureaucrates et les politiciens à élaborer de meilleurs programmes administratifs qui soient plus efficaces et moins draconiens.

Serions-nous déjà tombés si bas que nous sommes prêts à abandonner le fondement d'une société civilisée qu'est le respect des droits humains ? Mais il faudrait être naïf pour ne pas admettre que la menace est bien réelle.

Le défi, comme toujours, reste d'amener la société à constater le problème, et il y a de nombreux signes encourageants à ce chapitre. Plus d'un pays, y compris le Canada, s'activent déjà pour renforcer les droits de leurs citoyens de choisir et de contrôler leurs renseignements personnels. La Communauté européenne est déjà passée à l'action, et une partie de l'ancienne Europe de l'Est emboîte le pas. La Nouvelle-Zélande, Hong Kong et la Thaïlande ont adopté des lois protégeant la vie privéee, et l'Australie devrait suivre le mouvement. Ces initiatives témoignent assurément d'un désir accru des citoyens d'empêcher la technologie d'écraser leurs droits fondamentaux.

La vie privée est-elle morte? Certes, elle bat de l'aile, mais la lutte reste la façon éternelle et immuable de préserver toutes les libertés. Les libertés perdues ne peuvent être recouvrées qu'au prix d'énormes efforts et de grandes douleurs. Personne ne peut affirmer avec certitude que ce n'est pas le sort qui attend notre droit à une vie privée. Mais si la liberté parvient à survivre, il en sera de même pour la vie privée, car la liberté ne peut exister sans le droit à une vie exempte de surveillance et de dirigisme.

Le combat est loin d'être terminé. Comme le disait John Paul Jones, héros naval américain, la lutte ne fait que commencer.

Une longue route

Le Canada disposera bientôt d'une nouvelle arme dans sa lutte contre le problème des communications électroniques : un mélange de principes et de gestes concrets. Au chapitre des principes se retrouve notre désir de faire respecter des droits humains essentiels, et nos gestes concrets visent à faire du Canada un chef de file en matière de commerce électronique.

Lorsque le Parlement a ajourné pour l'été, le projet de loi C-54 sur la protection des renseignements personnels et les documents électroniques est resté en suspens. Ce projet vise à étendre la portée des lois fédérales sur la protection des renseignements personnels aux entreprises privées canadiennes (voir notre étude du projet de loi en page 97).

Si ce projet de loi est entériné, il constituera la plus grande étape franchie dans le domaine de la défense de la vie privée depuis l'adoption de la *Loi sur la protection des renseignements personnels* par le gouvernement fédéral en 1982.

Si le projet de loi n'est pas adopté, par contre, la population canadienne aura toutes les raisons du monde de se méfier tant de la façon dont les entreprises privées gèrent ses renseignements personnels que du principe même du commerce électronique. L'absence de tout droit juridique de contrôler la collecte et l'utilisation de nos renseignements personnels par ces entreprises mettra notre vie privée électronique à la merci des caprices des propriétaires des réseaux, et elle pourrait fort en souffrir si sa protection va à l'encontre de leurs pratiques commerciales.

Le projet de loi C-54 a, à juste titre, fait beaucoup parler de lui, et les audiences du comité de la Chambre des communes ont duré plusieurs mois. On a relevé deux types de représentations : celles des entreprises qui considéraient que le projet de loi est trop contraignant, et celles des groupes de défense des droits de la personne et des consommateurs, qui le trouvaient trop permissif. Un bon équilibre a peut-être été atteint.

Bien que loin d'être parfait (quel projet de loi l'est-il jamais?), ce projet de loi représente dans ses grandes lignes un grand bond en avant. Une fois pleinement en vigueur, il assujettirait les entreprises à un code de pratiques équitables exigeant le consentement de la personne pour la collecte, l'utilisation et la communication de ses renseignements personnels. De façon toute aussi importante, le projet de loi comporte un mécanisme de

surveillance indépendant qui confie au Commissariat fédéral à la protection de la vie privée le mandat d'étudier les plaintes, de rédiger des rapports et d'effectuer des vérifications. En dernier ressort, il permet à la Cour fédérale de réviser les enjeux soulevés et d'accorder des dommages-intérêts au besoin.

Le projet de loi témoigne de beaucoup d'ingéniosité et de courage. La plupart des activités commerciales au Canada relèvent de la compétence des provinces (à l'exception des opérations bancaires, des télécommunications et du transport interprovincial). Cependant, le gouvernement fédéral a le pouvoir constitutionnel de réglementer le commerce interprovincial et international. L'entrée en vigueur du projet de loi s'effectuera donc en deux étapes. D'abord, les activités commerciales réglementées par le gouvernement fédéral seront soumises au projet de loi un an après son adoption. Ensuite, trois ans plus tard, cette loi s'appliquera aux activités commerciales dans les provinces n'ayant pas adopté de loi comparable.

Bien que l'opération soit certes délicate, le gouvernement s'est employé à faire en sorte que chaque citoyen, où qu'il habite, jouisse de droits juridiques communs en matière de protection de ses renseignements personnels.

La même justice pour tous

Il faut également soulever le soulagement que ne manqueront pas de pousser les entreprises canadiennes à l'entrée en vigueur du projet de loi, dont les principes clé sont ceux du Code qu'a adopté l'Association canadienne de normalisation en matière de protection des renseignements personnels. Ce Code est en effet le fruit des efforts conjoints de ces mêmes entreprises et leur appartient en quelque sorte. En fait, ce code représente une certaine force morale au sein du secteur privé, ainsi que l'indiquait quelqu'un récemment. Le projet de loi devrait donc normaliser les pratiques de chaque entreprise, empêchant ainsi certains écarts de conduite dont pourrait souffrir l'ensemble du secteur privé.

La décision du gouvernement de continuer de faire appel à un ombudsman pour l'examen des plaintes est toute aussi réjouissante. Certains témoins ont fait valoir qu'un commissaire quasi judiciaire et émetteur d'ordonnances serait plus efficace. Mais le présent commissaire, convaincu que la négociation et l'éducation l'emportent sur des mesures coercitives rigides, n'est pas de cet avis, faisant valoir les 15 ans d'expérience du Commissariat en la matière. Ces 15 ans ont vu l'Ombudsman mettre l'accent non seulement sur le règlement des plaintes mais aussi sur la détermination et la résolution des problèmes les ayant provoquées.

En dernier ressort, il reste La Cour fédérale. Mais des 20 000 plaintes traitées par le Commissariat depuis 1983, moins d'une douzaine y ont abouti. Le Commissariat vise davantage à régler les problèmes qu'à jouer au policier, une approche d'autant plus nécessaire dans le secteur privé. Le monde des affaires est infiniment complexe; y faire irruption de manière arbitraire ou brusque compromettrait dès le départ les chances d'améliorer la protection des renseignements personnels.

L'objectif du projet de loi n'est pas de nuire aux entreprises mais bien de les aider tout en stimulant la confiance du public dans le commerce électronique. Le projet de loi vise à promouvoir un état d'esprit dans lequel les entreprises tiennent systématiquement compte des droits des clients, des consommateurs et des employés en matière de protection de leurs renseignements personnels au cours de la fabrication de leurs produits et de l'élaboration de leurs pratiques administratives. Cela suppose évidemment temps et patience, mais il ne fait aucun doute que les résultats seront extrêmement positifs. Les entreprises, bien plus que les bureaucraties gouvernementales, dépendent de la satisfaction des clients et des consommateurs. La réputation d'une entreprise est son bien le plus précieux; aucune ne souhaiterait être publiquement critiquée pour avoir délibérément bafoué des droits individuels.

Combattre l'ignorance

Une des composantes cruciales du projet de loi est la responsabilité qu'il confie au Commissariat de s'attaquer au plus grave problème auquel se heurte la protection de la vie privée au Canada : l'ignorance. En effet, le Commissariat se verra confier un mandat éducatif, dont les entreprises qui n'ont pas déjà commencé à le faire bénéficieront. Les consommateurs, quant à eux, voudront en savoir le plus possible sur leurs droits et leurs responsabilités, car plus ils en sauront, moins ils craindront l'inconnu et plus leurs décisions seront éclairées. Mais aucun mur ne peut tenir debout sans briques : l'éducation publique est essentielle, certes, mais elle exige des ressources, et notre Commissariat est au régime maigre depuis déjà plusieurs années (ne disposant même d'aucun budget de recherche et d'éducation). Bien que le Conseil du Trésor ait commencé à s'attaquer au problème de l'année dernière, élargir le mandat du commissaire au secteur privé nécessiterait beaucoup plus de briques.

Le projet de loi C-54 n'est pas la réponse à tous nos maux. De nombreux problèmes liés à la protection des renseignements personnels persistent. Les projets de surveillance continuent de se multiplier. Tous les gouvernements emploient des partisans d'un partage étendu et ininterrompu de

renseignements personnels entre ministères, paliers de gouvernement et secteurs public et privé au nom d'une efficacité administrative accrue. Selon ces partisans, une telle efficacité est primordiale, l'emportant sur tout, y compris notre droit de consentir de façon éclairée à la collecte et l'utilisation de nos renseignements personnels.

Il est possible que *The Economist* ait raison : les lois actuelles ou à venir ne suffiront peut-être pas à enrayer cette tendance accrue à surveiller les moindres faits et gestes de notre population. Le cas échéant, il faudra songer à d'autres moyens d'action, et les mettre en pratique. Mais il faut commencer quelque part, et la chose presse. Si les groupes de pression et les querelles de compétence nous ralentissent trop, cela signifiera la fin de la vie privée de nos citoyens et celle des initiatives commerciales électroniques.

Que penser du projet de loi C-54 ?

Des nombreuses critiques soulevées au sujet du projet de loi, certaines étaient de nature spécifique et technique. Nos commentaires détaillés quant au projet sont disponibles tant à nos bureaux qu'au site Web du Commissariat. Nous nous devons de nous pencher ici sur deux critiques en particulier, soient celles visant la non-application du projet de loi aux documents de nature journalistique, artistique ou littéraire, ni à ceux colligés aux fins de l'application de lois.

L'exclusion journalistique : Celle-ci nous touche de près, et vous devriez savoir que les commentaires suivants sont biaisés par les quelque trente ans de notre Commissaire actuel en tant que journaliste, une profession qui semble déplaire à beaucoup de gens mais dont la quasi totalité de la population reconnaît la nécessité. À preuve cette remarque de Thomas Jefferson, qui aurait sans hésiter choisi un pays doté d'une presse libre mais sans gouvernement à un pays où la situation aurait été inverse. Même les journalistes, cependant, ne disposent pas d'une liberté absolue.

Cette exemption a soulevé de nombreux débats au Parlement : certains députés croient fermement que les journalistes actuels envahissent par trop la vie privée des gens. Le comité de la Chambre des communes chargé de l'étude du projet de loi a demandé à notre Commissaire d'expliquer son soutien à cette exemption, lequel a souvent fait l'objet de questions par le passé.

Rappelons-nous une vérité fondamentale : il n'est pas du rôle des médias de protéger notre vie privée, car leur objectif premier est de recueillir et de diffuser des nouvelles. Les médias doivent cependant éviter de causer tout tort inutile en évitant de divulguer des détails d'un goût douteux.

Les journalistes ont de grandes responsabilités, car nul ne tient plus à autre chose qu'à sa bonne réputation. Compromettre cette dernière pour le simple plaisir d'émoustiller ou de divertir la population est un geste dont les conséquences peuvent durer toute une vie. Les sommes d'argent accordées par les tribunaux, si substantielles soient-elles, ne suffisent pas à restaurer la réputation d'une personne (et que dire de tous ceux qui n'ont même pas les moyens d'entamer des poursuites devant les tribunaux?).

Les grands médias canadiens actuels récoltent généralement de bonnes notes (quoi qu'en disent certains). On se rappelle certes quelques exceptions tout autant mémorables que déplorables, mais le Canada n'a encore jamais connu le genre de harcèlement médiatique qui est le lot de la famille royale britannique. Les personnalités publiques devraient bien sûr s'attendre à moins de vie privée, mais beaucoup ne s'en plaignent pas puisque l'attention publique contribue à leur carrière.

Le fait d'assujettir des journalistes à une loi qui exigerait qu'ils obtiennent le consentement de tout un chacun à la collecte de ses renseignements personnels reviendrait cependant à compromettre leur travail. Ce dernier, pour aussi impopulaire qu'il soit à l'occasion auprès de certains, est indispensable dans une société libre que reconnaît notre *Charte canadienne des droits et libertés*.

L'exclusion visant les forces de l'ordre : Nous ne pouvons passer sous silence le nouveau succès que les groupes de pression d'Ottawa représentant les forces de l'ordre a obtenu auprès du gouvernement, persuadant ce dernier d'accorder aux corps policiers une exclusion excessivement permissive du champ d'application du projet de loi. En fait, il s'agit bien plus que des corps policiers, puisque l'exclusion s'applique également à toute personne ou agence administrant des lois telles la *Loi de l'impôt sur le revenu* ou la *Loi sur l'assurance-emploi*. Cette exclusion s'applique à toute enquête reliée à ces lois, permettant aux entreprises privées de ne pas dire à un citoyen qu'un policier ou un fonctionnaire a demandé accès à ses renseignements personnels si le policier ou le fonctionnaire s'y oppose. Une telle restriction se défend tant et aussi longtemps que la divulgation compromettrait une enquête en cours. Mais une fois celle-ci terminée, il n'y a souvent aucune raison de ne pas aviser

le citoyen de ce qui est survenu à ses renseignements personnels, surtout dans le cas d'enquêtes de nature administrative.

Le projet de loi C-54 donne cependant aux forces de l'ordre une latitude absolue à ce chapitre, lesquelles n'ont aucunement besoin de prouver que la divulgation au citoyen compromettrait leur enquête. De plus, contrairement aux dispositions actuelles de la *Loi sur la protection des renseignements personnels*, le projet de loi C-54 n'oblige nullement les entreprises à noter les communications qu'elles font aux forces de l'ordre afin de permettre à notre Commissaire d'en évaluer la pertinence. Une telle obligation s'est avérée salutaire dans l'appareil gouvernemental fédéral, permettant un suivi des enquêtes.

Il reste que les entreprises privées ne sont tenues de communiquer les renseignements demandés aux forces de l'ordre que si ces dernières disposent d'un mandat en bonne et due forme. Un tel mandat n'étant pas requis pour la plupart des demandes de nature administrative (bien que la demande doive habituellement se conformer à un règlement quelconque), il serait donc d'autant plus logique d'exiger des comptes des parties en cause.

Nous ne pouvons passer sous silence le fait que la *Loi sur la protection des renseignements personnels* permette également aux forces de l'ordre de refuser sans motif à un citoyen de consulter le dossier d'une enquête le concernant. Nous nous sommes déjà prononcés contre une telle latitude, et redoublerons d'efforts à ce chapitre, ce sujet faisant partie des principales modifications dont la *Loi sur la protection des renseignements personnels* a grand besoin depuis un certain nombre d'années.

Ces modifications prennent par ailleurs une importance accrue dans le cadre de l'entrée en vigueur prévue du projet de loi C-54 : les deux textes législatifs diffèrent en effet substantiellement à certains égards, et devraient donc être accordés. À titre d'exemple, la *Loi sur la protection des renseignements personnels* ne permet le recours à la Cour fédérale que suite à un refus de communication de renseignements personnels, alors que le projet de loi C-54 rajoute entre autres à ceci la révision de plaintes de collecte, d'utilisation et de divulgation abusives de renseignements, la base de tout code de protection de la vie privée. Une telle différence mènerait, si elle était maintenue à l'établissement par le Parlement d'une norme de protection de la vie privée qui serait inférieure au sein de l'appareil gouvernemental fédéral que ce qu'elle serait dans le reste du pays. Une situation difficilement défendable...

Infostructure de la santé = surveillance ?

Des progrès ont été enregistrés cette année au chapitre de la protection des renseignements personnels sur la santé. Les propositions relatives à la création d'un réseau national de renseignements sur la santé, dévoilées dans le budget de 1997, offraient des perspectives intéressantes pour l'amélioration de la santé au pays et du système canadien de soins de santé. Elles présentaient également, toutefois, des risques considérables en matière de protection du caractère confidentiel des données relatives aux patients si elles ne sont pas assorties de strictes mesures de protection. Comme il était mentionné dans notre rapport annuel de 1996-1997 : "Une collecte et une circulation accrues de renseignements médicaux ne peuvent qu'alarmer au chapitre de la vie privée".

Nous avons suivi de près l'évolution de ce dossier et rencontré des responsables de Santé Canada. Nous avons aussi indiqué aux membres du Conseil consultatif sur l'infostructure de la santé de laisser à l'ordre du jour la question de la protection de la vie privée, et fourni à ceux-ci des commentaires sur les versions provisoires et définitive de leur rapport.

Le rapport final : En février, le Conseil consultatif sur l'infostructure de la santé publiait son rapport final, lequel semblait reconnaître l'importance critique des questions relatives à la protection des renseignements personnels dans la mise sur pied d'une telle infostructure. Le rapport mentionnait la protection de la vie privée comme l'un des quatre objectifs stratégiques à atteindre dans la création du réseau. Il reconnaissait également l'importante distinction à établir entre la protection de la vie privée des patients, ce qui signifie que certains renseignements les concernant ne seront pas recueillis, et la sécurité à apporter aux renseignements de ces derniers. Le Conseil a également souscrit à l'adoption de dispositions législatives spécifiques à la protection des renseignements personnels sur la santé et en a énoncé les éléments essentiels. De plus, le Conseil s'est dit en faveur de l'harmonisation de la protection des renseignements personnels partout au pays, tout en recommandant d'éviter de s'en tenir au plus petit dénominateur commun.

Tout cela est bien beau, mais d'autres messages importants semblent avoir été oubliés. Le premier est l'apparente incapacité du rapport à reconnaître au patient le droit de refuser de prendre part à tout réseau national de surveillance des renseignements sur la santé. En outre, le rapport n'établit pas de limites à la surveillance individuelle que subiraient les patients qui choisissent de participer au réseau.

Le fait que le rapport reconnaisse que des groupes de personnes peuvent être stigmatisés par l'utilisation de données sur la santé en leur défaveur représente un autre jalon important. Malheureusement, cette reconnaissance se limite aux Autochtones et aux communautés culturelles. Pourtant, n'importe quel groupe de personnes peut être perçu comme présentant des caractéristiques particulières qui sont par la suite attribuées, à tort ou à raison, à chaque membre du groupe. Cette conclusion peut s'avérer simpliste et dangereuse. La notion de protection de la vie privée "collective" mérite une interprétation plus large dans le contexte des soins de santé et, de façon générale, une plus grande attention.

Le rapport écarte également sans ménagement une autre recommandation du Commissariat, soit celle voulant que les conseils de recherche et d'examen de la déontologie comprennent des défenseurs de la vie privée ou des droits des patients. Faute d'un "avocat" des droits individuels, la notion de "l'intérêt public" ou, peut-être, d'une "plus grande efficacité" aura inévitablement préséance. Le fait de permettre aux responsables et aux chercheurs du secteur de la santé de défendre les intérêts des patients équivaudrait à confier la garde du poulailler à un certain colonel.

Le ton du document complémentaire intitulé *Carnet de route de l'information sur la santé*, qui a été produit par Santé Canada, Statistique Canada et l'Institut canadien d'information sur la santé, ne peut qu'entretenir notre inquiétude. Si ce document doit servir de plan directeur pour la mise en application du rapport, alors il y manque des pages importantes.

Le Carnet de route de l'information sur la santé : Ce Carnet décrit les étapes menant à la mise sur pied d'un réseau global de renseignements sur la santé qui permettrait d'offrir des soins aux particuliers. Bien que le Carnet reconnaisse aux individus d'importants droits sur la fréquence et les modalités entourant l'utilisation de leurs renseignements médicaux, il n'offre à ces individus que deux solutions. La première, peut-être plus décorative qu'utile, permettrait aux patients d'obtenir copie des politiques des organismes en matière de respect de la vie privée. La seconde, qui dissocierait le nom d'un patient de son dossier médical, ne viserait que la confidentialité des renseignements, et non la vie privée du patient.

Et cette vie privée est clairement en jeu. Le plus blasé des lecteurs ne pourrait s'empêcher de sursauter à la lecture de la proposition que fait le Carnet de route de suivre chacun des gestes posés par un patient au sein du système de santé au cours d'une longue période de temps. Que dire aussi du

besoin de plus de renseignements personnels dont le Carnet fait état, ainsi que de la nécessité d'en élargir l'éventail? Les autres renseignements personnels qui seraient ainsi visés touchent notamment à l'état de santé et aux facteurs autres que médicaux affectant ce dernier. Ce côté "surveillance" se reflète clairement dans la proposition d'un Réseau national de surveillance sur la santé.

Le Réseau national de surveillance sur la santé : Il existe évidemment un besoin de suivre certaines situations ou personnes afin de protéger la population de tout danger immédiat que poserait, par exemple, une maladie infectieuse ou un pesticide dangereux. Dans sa plus récente version, cependant, le réseau semble désormais destiné à promouvoir la santé et le bien-être. Les partisans de la surveillance de la population paraissent vouloir appliquer à ce dernier objectif les mêmes raisons importantes qui visaient la protection du public, un but pourtant complètement différent.

Le suivi longitudinal proposé dans un document de travail de Santé Canada toucherait à l'éventail complet des rôles déterminés par la société, aux composantes de la personnalité, aux attitudes et comportements, aux valeurs, au pouvoir relatif et à l'influence qui caractérisent l'existence de nos citoyens. Un tel suivi serait une incroyable intrusion, d'une ampleur renversante et porterait atteinte au droit fondamental à une vie privée que garantit toute démocratie. Tout réseau sur la santé devrait permettre à n'importe quel patient de se soustraire à une telle surveillance sans pour autant compromettre ses soins de santé. Il semble que les défenseurs d'un tel réseau

ont, une fois de plus, confondu la notion d'une bonne sécurité avec celle de la protection de la vie privée. Le consentement éclairé est un principe trop fondamental pour être ainsi ignoré.

La plus grande faiblesse du rapport, des documents de recherche et du Carnet de route tient dans le manque de précisions sur la façon dont circulera l'information. Il n'y a en effet aucun diagramme expliquant la manière dont et le lieu où les données sur la santé seront reliées, l'ampleur des détails personnels visés ou les personnes qui y auraient accès. Sans de telles précisions, les fournisseurs de soins de santé, les fonctionnaires, les patients et les défenseurs du respect de la vie privée ne sont pas en mesure d'établir à quoi tiennent les risques et les moyens d'éliminer ceux-ci.

En fait, le manque de précisions constitue en soi une source de désaccord entre les intervenants. Par exemple, le Conseil a déjà protesté à plusieurs reprises contre le fait que rien n'a été prévu en vue de la création d'un dossier du patient qui soit intégré. Pourtant, le Carnet de route de l'information sur la santé parle d'un "système de santé intégré, où les patients peuvent aller sans problème d'un hôpital à un établissement de soins prolongés, à des soins à domicile ou à d'autres milieux, selon leurs besoins" et d'un "dossier médical intégré (au niveau régional ou local)". Le document poursuit en parlant de recueillir "des données plus détaillées sur des groupes ou des personnes spécifiques" et de "travailler avec toutes les provinces pour faciliter une éventuelle *centralisation* [emphase mise dans le document original] de l'information contenue dans leurs systèmes de dossiers basés sur la personne".

Il n'est guère difficile de conclure que l'infostructure sur la santé propose en fait l'intégration massive de profils de patients identifiés par leur nom, qui soient accessibles à l'échelle nationale par tout un éventail de fournisseurs de soins, de chercheurs et de fonctionnaires. Il est peu rassurant d'entendre les défenseurs d'un réseau sur la santé parler de réseaux distribués au lieu de bases de données centralisées de renseignements sur les patients. Il s'agit là d'une distinction sans différence. Peu importe que les renseignements se retrouvent dans une seule base de données ou soient accessibles en direct sur un réseau, car trop de personnes y auront accès dans l'un ou l'autre des cas. La protection de ces renseignements dépendra de la quantité et de la solidité des mécanismes de contrôle qui régiront leur disponibilité. La protection de la "vie privée" des patients en remplaçant les noms de ceux-ci par des numéros représente une solution simpliste à un problème complexe. Il est en effet très simple de retrouver l'identité de ces personnes et, ce faisant,

d'obtenir la clé d'un dossier personnel exhaustif et extrêmement détaillé. Et quelles autres personnes viendront se mettre à la suite des autres pour dire qu'il leur faut consulter ces documents? Les forces de l'ordre? Les services de la sécurité sociale? Les fonctionnaires des services de l'emploi et des pensions?

Certes, nous pouvons comprendre que les travaux en sont à leurs débuts, et que les infrastructures varient d'une province à l'autre, mais il semble inconcevable que les divers projets pilotes en cours aient pu avancer à ce point sans que l'on tente de définir les échanges d'information. Les dénégations contribuent à entretenir le doute au sujet du projet de réseau. Il est temps que les responsables détaillent leurs propositions et permettent à la source de toutes ces précieuses données, soit le patient, de participer au débat de fond.

Les législateurs qui sont à la recherche de conseils en vue de l'élaboration de dispositions sur la protection des renseignements personnels sur la santé n'ont pas besoin de réinventer la roue : le Code de protection des renseignements de santé de l'Association médicale canadienne représente un excellent repère pour l'atteinte d'un niveau national élevé de protection des renseignements relatifs aux patients. Le Code pourrait servir de base à un projet de loi. Vu les lamentations selon lesquelles le Code place la barre trop haut, peut-être qu'une partie des fonds qui ont été accordés à l'équipe de l'infostructure de la santé devrait servir à financer une étude sur les conséquences de la mise en œuvre du Code. Les patients méritent bien çà.

La santé en Saskatchewan

La nouvelle *Health Information Protection Act* (loi sur la protection des renseignements sur la santé) de la Saskatchewan, qui a reçu la sanction royale au début de mai, garantit une plus grande transparence des méthodes de la province en matière de gestion de renseignements sur la santé tout en permettant aux patients d'exercer un certain contrôle à l'égard de leurs propres renseignements. Comme l'a dit un journaliste local : "Je trouve foncièrement réconfortant de voir que le berceau canadien de la médecine socialisée est également la première province à accorder à ses citoyens le droit de refuser de communiquer aux fonctionnaires le dossier détaillé de leur état de santé, même si ce droit doit être exercé par le biais d'une démarche expresse de la part des citoyens." [traduction]

Certains des principes qui sont énoncés dans le préambule sont notamment extraits du Code de protection des renseignements personnels sur la santé de

l'Association médicale canadienne. Les patients ont le droit d'interdire que soit versé au réseau provincial d'information sur la santé ou à tout autre réseau prévu par règlement tout renseignement personnel qu'ils ont confié à leur médecin. De plus, le patient peut demander à un "fiduciaire" (c'est-à-dire tout individu ou organisme détenant des renseignements médicaux) de limiter à tout autre fiduciaire l'accès à une partie ou la totalité des renseignements versés au réseau. Et l'article 9 exige des fiduciaires qu'ils sensibilisent les patients aux droits que leur confère la nouvelle loi.

Les sanctions prévues en cas de contravention à la loi font passer le bon message. Ainsi, tout individu surpris à obtenir des renseignements de santé de façon illégale est passible d'une amende pouvant atteindre 50 000 $, ou dix fois plus dans le cas d'une entreprise.

La loi contient toutefois des dispositions inquiétantes. Par exemple, la définition qu'on y donne d'un "fiduciaire" est très vaste et peut s'appliquer à presque n'importe qui. Il n'existe aucune distinction entre les médecins, les organismes gouvernementaux ou les entreprises qui fournissent des soins de santé en vertu d'un accord conclu avec un autre fiduciaire. De plus, la loi ne s'applique pas aux renseignements statistiques ou soi-disant dépersonalisés », soient ceux dont le nom du patient a été remplacé par un code. Une telle substitution d'un code ne rend nullement les renseignements anonymes, puisque le système peut toujours associer les renseignements au patient qu'ils concernent.

La loi prévoit également une longue liste de fins secondaires pour lesquelles les renseignements personnels de santé d'un patient peuvent être communiqués sans son consentement : si la santé de quiconque (dont le patient) est menacée, pour dépister et suivre les cas de fraude, ou encore pour permettre aux comités de surveillance de contrôler la qualité des services de santé. Le gouvernement s'est par ailleurs donné une marge de manœuvre considérable en s'octroyant de vastes pouvoirs de réglementation dans diverses dispositions de la nouvelle loi.

Tout cela pour dire que plusieurs questions restent sans réponse, même si nous faisons montre d'un certain optimisme quant à la protection que la loi accorde aux patients. Par exemple, quels critères utilisera-t-on pour déterminer qui peut devenir fiduciaire ? Et les membres des comités d'éthique en matière de recherche comprendront-ils un représentant des droits des patients ou un défenseur de la vie privée ?

Le NAS pris au sérieux

Le Vérificateur général confirme les assises fragiles du NAS

Les lecteurs de rapports antérieurs n'ignorent pas que les utilisations légitimes comme abusives du désormais tristement célèbre numéro d'assurance sociale (NAS) suscitent l'intérêt constant du Commissariat, et parfois des bâillements prévisibles chez d'autres organismes. Deux camps s'opposent dans ce débat, soit les personnes qui voient dans l'utilisation croissante du NAS une tendance dangereuse pouvant mener à la création de bases de données intégrées et à l'adoption d'une carte d'identité nationale, et d'autres gens pour qui ces craintes ne sont que des réactions irrationnelles à l'égard d'un numéro de dossier national.

Le plus grand risque posé par le NAS a toujours été celui qu'il devienne un code d'identification national et, par conséquent, une clé donnant accès à des renseignements personnels contenus dans des systèmes d'information de plus en plus reliés. Cela représente un risque sérieux pour un numéro que traitent avec autant de désinvolture le gouvernement, les entreprises et les particuliers.

La dénonciation la plus récente et, pourrait-on dire, la plus vigoureuse, du problème du NAS vient d'une source peut-être surprenante : le Vérificateur général. Que le Commissaire à la protection de la vie privée déclare que le NAS fait problème n'a pas de quoi étonner. Mais lorsque le Vérificateur général, avec son mandat incisif (et les ressources permettant la tenue d'enquêtes approfondies) conclut que la façon dont le numéro d'assurance sociale est géré pave la voie à la fraude et aux intrusions dans la vie privée, des signaux d'alarme retentissent.

Force est de souligner que toutes les recommandations du VG ne font pas l'affaire d'un commissaire à la protection de la vie privée : après tout, les centres d'intérêt du VG sont l'économie et l'efficience financière gouvernementales. Néanmoins, nous nous réjouissons que le numéro d'assurance sociale et son système de soutien reçoivent enfin l'attention rigoureuse qu'ils méritent.

L'enquête du Vérificateur général portait sur "la gestion et le contrôle du NAS pour déterminer s'ils sont efficients et efficaces et s'ils ont un fondement approprié dans la législation".

Le Vérificateur général a conclu que le NAS "est devenu un code d'identification national de fait dans les transactions relatives au revenu, contrairement à l'intention du gouvernement". Malgré les mesures prises par ce dernier pour limiter ses propres utilisations du NAS à la suite de l'examen triennal de la *Loi sur la protection des renseignements personnels*, les changements qui ont été apportés en 1992 à la *Loi de l'impôt sur le revenu*, nécessitant l'inscription du NAS sur les prestations d'aide sociale et les indemnisations aux victimes d'accidents du travail, ont ouvert tout grand la porte.

"Cette exigence assurait, à toutes fins pratiques, la prédominance du NAS comme code d'identification commun pour les programmes sociaux des provinces et des municipalités", a conclu le Vérificateur général. Avec les programmes sociaux fédéraux, le VG a évalué à près de cent milliards de dollars par année les dépenses sociales gouvernementales. Comme "de nos jours, le NAS est exigé pour à peu près toutes les transactions touchant un prêt ou un paiement de soutien du revenu, la perception des recettes et les finances personnelles", les couplages de données deviennent extrêmement attirants. Même lorsque le taux d'usage frauduleux n'est que de un à quatre pour cent, les avantages des couplages sont trop tentants pour les décideurs, suffisamment en tous cas pour balayer les principes déontologiques et les obstacles juridiques du revers de la main.

Le VG a également trouvé que le Registre d'assurance sociale comprenait quelque 3,8 millions de détenteurs de NAS de plus que de résidents canadiens âgés de 20 ans et plus. Voilà qui remet en cause l'exactitude de la base de données appuyant le système, et qui ouvre la porte à cette menace croissante qu'est le vol d'identité dans une société de l'information. Et avec la nouvelle Subvention canadienne pour l'épargne études, un million d'enfants viendront joindre les rangs des détenteurs d'un NAS, et ce même si les conséquences fiscales ne se concrétiseront pour eux que lorsqu'ils commenceront à retirer des fonds du régime.

Amélioration du Registre : Trois des recommandations faites par le Vérificateur général appellent une réponse du Commissaire à la protection de la vie privée. La première vise une intégrité accrue du registre, et le VG a proposé le resserrement du processus de vérification de l'identité des demandeurs de NAS : par exemple, un répondant admissible pourrait devoir signer la demande, un peu comme dans le cas des passeports. Le VG a aussi recommandé que l'on procède à une vérification des certificats de naissance des demandeurs auprès des registres de l'état civil des provinces, desquels

seraient également obtenus les noms des personnes décédées, dont le NAS serait alors rayé. D'aucuns estiment que les décès qui ne sont pas déclarés sont la principale cause des millions de numéros d'assurance sociale en trop.

Manifestement, le Registre a besoin d'un bon nettoyage. Comment devrait-on y procéder? Il semble que la pièce d'identité la plus probante, le certificat de naissance, ne fasse malheureusement plus l'affaire de nos jours. Étant donné que ces certificats sont parfois des faux, il semble désormais préférable de les confirmer auprès l'organisme qui les a émis. Cela n'a rien de compliqué s'il s'agit seulement de confirmer les renseignements de base. Cela le devient, cependant, lorsque le registre de l'état civil lui-même contient peut-être des renseignements superflus comme ceux supposément inscrits dans le registre de l'Alberta (renseignements sur le mode de vie de la mère: consommation de tabac, de drogue et d'alcool).

Ces renseignements satisfont peut-être la curiosité de certains fonctionnaires, mais ils ne contribuent guère à accroître l'exactitude du Registre de l'assurance sociale. Cet exemple met en lumière l'importance cruciale de limiter l'accès du gouvernement fédéral à l'information de base absolument requise pour confirmer l'identité des demandeurs et supprimer les noms des personnes décédées.

Parmi les autres facteurs contribuant au nombre excédentaire de NAS par rapport à la population, mentionnons la série des 900, ces NAS dits temporaires commençant par "9" qui sont attribués aux résidents non permanents (comme les demandeurs du statut de réfugié, les travailleurs saisonniers et les étudiants étrangers). En 1998, 680 000 de ces numéros temporaires étaient actifs, dont 66 p. 100 depuis plus de cinq ans. Un bon nombre de détenteurs de ces NAS peuvent avoir tout simplement oublié de prévenir le gouvernement de leur départ; d'autres, par contre, pourraient se trouver au Canada illégalement. La suggestion du VG concernant l'émission de NAS de série 900 avec une date de péremption semble juste et logique, vu leur nature temporaire.

La proposition voulant donner aux responsables du Registre et à Revenu Canada accès aux dossiers des clients de Citoyenneté et Immigration soulève quant à elle certains problèmes. Cet accès permettrait respectivement de confirmer le statut des intéressés et de vérifier si le NAS est actif. Nous pouvons comprendre que Citoyenneté et Immigration doive informer le Registre de tout changement dans le statut d'un client (obtention du statut d'immigrant reçu, déportation, etc.), mais pas que les responsables du

Registre mettent systématiquement leur nez dans les dossiers de l'immigration.

Nous ne pouvons pas accepter non plus que les administrateurs du Registre aient accès aux dossiers de n'importe quel organisme gouvernemental inscrivant le NAS dans ses dossiers pour vérifier si tel ou tel numéro est encore actif. Un accès aussi illimité risque en effet de mener le Registre à progressivement accumuler quantité de renseignements sur les transactions entre le détenteur d'un NAS et le gouvernement. Ces données détourneraient le Registre de sa fonction première pour en faire un méga entrepôt de données propice au couplage de renseignements.

Un Registre plus exact et le resserrement des preuves d'identité contribueraient grandement à en corriger les inexactitudes et à prévenir les utilisations frauduleuses et abusives.

Intégration de dispositifs de vérification dans la carte : Le VG soutient de plus que la carte d'assurance sociale devrait quant à elle offrir davantage d'information pour confirmer que la personne qui la présente en est bien le détenteur légitime. Parmi les options, mentionnons une photographie, une signature électronique et un code d'identification biométrique tel un balayage de la rétine ou de la forme de la main.

C'est à ce point-ci, des plus dangereux, que le NAS, simple numéro de dossier d'un client, devient un véritable identifiant sur carte. Aucun commissaire à la protection de la vie privée ne peut accepter qu'un tel pas soit franchi.

Les cartes d'identité, même celles qui sont conçues à des fins précises, ont tendance à engendrer des caractéristiques secondaires indésirables. Même si la carte n'est pas nécessaire pour l'obtention d'un service, le fait d'en montrer une vient à s'inscrire rapidement dans les méthodes du service en question, et la carte finit par devenir obligatoire. Le fait de ne pas en avoir une ou de ne pas porter sa carte sur soi engendre des soupçons et, probablement, le refus du service en question.

La carte, parce qu'elle est considérée comme exacte et sûre, prend en soi une importance croissante. D'autres organismes gouvernementaux en quête de pièces d'identité fiables suivent le mouvement, et graduellement, la carte d'assurance sociale devient inévitablement une carte d'identité gouvernementale. Suivant les traces d'un utilisateur si important, le secteur

privé ne tarde pas à joindre les rangs sans cesse croissants de ceux qui exigent la carte. Et celle-ci devient un passeport national interne sans lequel vous n'êtes rien.

De plus, avec une pièce d'identité aussi fiable, l'utilisation du NAS ne pourra que croître. Et une utilisation élargie augmente le risque que le gouvernement et les entreprises aient accès aux renseignements vous concernant, où et quels qu'ils soient, et ce à votre insu et sans votre consentement. Un plus grand nombre d'utilisateurs et une utilisation accrue permettent inévitablement le couplage de davantage de données, menant au danger inhérent de l'établissement de profils. Et des profils détaillés réveillent généralement le spectre d'organisations anticipant, manipulant et programmant les comportements des particuliers.

Tous ces risques sont aggravés par le fait qu'il n'existe presqu'aucune limite quant aux circonstances permettant à un organisme de demander et d'utiliser votre NAS.

S'il est difficile de s'opposer à une carte d'assurance sociale qui soit plus exacte et plus sûre, il est plus urgent et plus utile de se demander quelle serait son utilité dans les millions de transactions que la population n'effectue pas en personne auprès d'un organisme gouvernemental (qu'il s'agisse, par exemple, de remplir une déclaration d'impôt ou de demander des prestations en vertu du Régime de pensions du Canada). Ces transactions "impersonnelles" constituent probablement la majorité de nos contacts avec le gouvernement. Le point faible du NAS est aussi son point fort car le numéro peut être utilisé (à bon ou à mauvais escient) dans des documents, au téléphone, voire, un jour peut-être, par ordinateur. Et l'intégration de dispositifs de sécurité à la carte ne sera en soi guère utile.

Nous souscrivons à l'appel du VG en faveur du resserrement du processus de vérification de l'identité pour l'émission d'un NAS et de la présentation d'autres pièces d'identité dans les transactions en personne. Selon le VG, toute personne possédant un NAS devrait présenter d'autres pièces d'identité. Un examen plus rigoureux des demandeurs pourrait accroître la confiance en ce numéro. Mais que faire des 33 millions de numéros qui sont déjà en circulation?

Réforme stratégique et juridique : La population ne peut presque pas se défendre contre les pressions croissantes qui souhaitent un plus grand partage des données personnelles. L'utilisation du NAS pour la collecte de renseignements personnels auprès de tous les utilisateurs autorisés pourrait

conduire à l'établissement de profils secrets détaillés sur de nombreux individus. Tous les mauvais usages actuels du NAS seraient exacerbés. Si la détection et la prévention des détournements de fonds publics représentent une bonne cause, elles ne justifient cependant pas pour autant que chaque citoyen se voie emprisonné dans une camisole de force électronique. Il doit y avoir un meilleur moyen.

Avant de me dire les jouets que tu veux, j'ai besoin de savoir tous tes prénoms et ton nom de famille, ton âge, ton adresse, le travail de tes parents, leur salaire et leurs biens. Et pour m'assurer que tu as vraiment été un bon petit garçon, il me faut aussi deux ou trois cheveux et une petite bouteille de ton pipi.

Le gouvernement pourrait commencer par suivre les conseils qui lui sont donnés régulièrement depuis plus de quinze ans : énoncer dans une loi les organismes habilités à demander le NAS et la façon d'utiliser celui-ci, interdire tout autre usage, et prévoir des sanctions contre les contrevenants. Le gouvernement ne peut pas envisager d'élargir ou de généraliser l'utilisation du NAS sans donner à celui-ci un cadre juridique.

Le NAS ne devrait pas non plus servir à accroître les échanges d'information tant que le gouvernement n'aura pas légiféré sur le couplage de données. La *Loi sur la protection des renseignements personnels* ne prévoit rien à cet égard, et la politique du Conseil du Trésor sur le couplage de données est davantage

ignorée que suivie. Le Vérificateur général souligne la nécessité de clarifier les règles et les rôles des parties dans l'exercice du contrôle et des responsabilités. Pour avoir maintes fois fait les mêmes exhortations, le Commissaire à la protection de la vie privée ne peut qu'applaudir. Il y a toutefois un problème, et de taille : la corruption du NAS, que présente le rapport du Vérificateur général. Allons-nous ériger un nouveau système sur de telles bases ?

Au-delà du simple numéro

L'automne dernier, deux comités permanents de la Chambre des communes ont suivi l'exemple du Vérificateur général et se sont penchés sur le NAS. C'était le Comité sur le développement des ressources humaines et le statut des personnes handicapées, et le Comité sur les comptes publics. Aucun de leurs membres ne souhaitait répéter le travail du VG, mais tous ont conclu que l'amélioration de la gestion actuelle du NAS ne représentait qu'une petite partie de la question : en effet, le gouvernement doit maintenant s'attaquer au plus gros et déterminer l'avenir du NAS. Le Comité sur les comptes publics perçoit la résolution du mandat du NAS comme une question de nature politique dont la réponse devra venir du Parlement canadien.

Dans son rapport final, le Comité sur le développement des ressources humaines souscrit à plusieurs des recommandations du VG quant à la gestion actuelle du NAS. Malgré de nombreux témoignages, cependant, les membres du comité ont conclu qu'ils n'avaient pas disposé d'assez de temps pour se pencher sur le cœur du problème, soit les enjeux stratégiques fondamentaux que sont la protection de la vie privée et le couplage de données, deux questions essentielles à l'avenir du NAS.

Un ancien comité de la Chambre, le Comité permanent sur les droits de la personne, s'était pourtant penché en 1997 sur ces mêmes enjeux. Suite à la dissolution du Parlement cette même année, son rapport, intitulé *La vie privée : où se situe la frontière?*, était resté sans réponse. Le Comité actuel sur le développement des ressources humaines a donc décidé de ne pas abandonner un tel effort, et a incorporé à son rapport final celui de l'ancien comité, le faisant sien et demandant au gouvernement une réponse formelle aux recommandations qu'il contient.

Le rapport du Comité actuel sur le développement des ressources humaines contient quant à lui plusieurs recommandations touchant au contexte élargi du NAS. Les membres du comité ont notamment demandé au gouvernement de légiférer les usages du NAS et les sanctions à imposer aux

contrevenants, faisant ainsi écho aux trois premiers Commissaires fédéraux à la protection de la vie privée et au rapport parlementaire ayant conclu la révision triennale de la *Loi sur la protection des renseignements personnels*. Après tout, qui peut rester patient après presque 20 ans d'attente?

Le comité a imposé trois dates butoir. Le ministère fédéral du Développement des ressources humaines a jusqu'au 30 septembre de cette année pour expliquer, tant aux membres du comité qu'à notre Commissariat, la progression des activités prévues en 1998-99 pour l'amélioration de la gestion du NAS.

D'ici à cette même date, le ministère devra également soumettre au Commissaire fédéral à la protection de la vie privée un rapport détaillant le projet pilote de mise à jour du Registre du NAS avec la collaboration de la Direction de l'état civil du Nouveau-Brunswick. Le Commissaire disposera alors de 30 jours pour faire parvenir son évaluation du projet pilote aux membres du comité de la Chambre.

D'ici le 31 décembre, le ministère devra également fournir aux membres du comité une analyse des options visant l'amélioration ou le remplacement du NAS par un tout nouveau système de carte, ainsi que de leurs coûts. Et c'est ceci qui compte vraiment. Tel que le rapportait le comité, trop de décisions passées reliées au NAS ont été prises sans réflexion. Le Commissaire prévoit déposer auprès du comité un document expliquant sa position sur les systèmes d'identification par carte, espérant ainsi aider les membres du comité tout en contribuant au débat de fond.

Les sciences sociales mènent le bal

Recensement de 1911

Les nouvelles selon lesquelles les formulaires remplis du recensement de 1911 ne seraient pas rendus publics ont voyagé à la vitesse de l'éclair au sein des communautés des historiens et des généalogistes. Le Commissaire à la protection de la vie privée a été l'une des parties qui ont été blâmées par les intéressés, et les lettres et les messages par courrier électronique ont afflué.

Il est vrai que le Commissaire à la protection de la vie privée avait de sérieuses réserves au sujet de la promesse de confidentialité absolue faite par Statistique Canada à l'égard des données du recensement, lesquelles finissaient ensuite par être connues par l'intermédiaire des Archives nationales. Après son enquête relative aux plaintes déposées au sujet du recensement de 1992, et en réponse aux préoccupations croissantes du public à l'égard des questions de plus en plus indiscrètes (particulièrement celles du formulaire long), le Commissaire avait recommandé que soient détruits les formulaires portant le nom des répondants. Même si Statistique Canada n'a que faire de ces formulaires une l'information vérifiée et consignée (sans les noms) dans des systèmes informatiques, les Archives nationales se sont opposées à leur destruction.

Cependant, les réserves du Commissaire ne représentent pas la raison fondamentale du refus de Statistique Canada de donner accès aux données du recensement de 1911. En fait, le règlement de la *Loi sur la protection des renseignements personnels* permet aux Archives nationales de transmettre les formulaires et les résultats de recensements après 92 ans aux fins de recherche et de statistique. L'obstacle à l'accès provient plutôt de la *Loi sur le recensement et la statistique* (de 1906) et plusieurs lois subséquentes qui empêchent Statistique Canada de communiquer les données de recensements à qui que ce soit , y compris aux Archives nationales.

Les motifs qui se rattachent à une protection aussi stricte sont clairs : nous sommes légalement obligés de répondre aux questions du recensement. À mesure que la société devient plus complexe, les questions se font plus détaillées et plus délicates et, peut-on soutenir, vont au-delà du simple relevé de la population. Parmi les questions figurant au questionnaire du dernier recensement, mentionnons celles portant sur la richesse et le revenu personnels, la religion, la fertilité et les déficiences physiques et intellectuelles.

La version d'essai du formulaire pour le recensement de 2001 comprend une question sur les partenaires de même sexe. Et avant chaque recensement, les gouvernements, les universitaires et les groupes d'intérêt tentent par tous les moyens que soient demandés le plus de renseignements possibles.

Sans conteste, les données du recensement représentent une ressource énorme et précieuse pour les gouvernements et les entreprises d'aujourd'hui. Mais lorsque les citoyens et les citoyennes sont obligés par la loi de communiquer des renseignements personnels, il incombe au gouvernement de protéger l'information, faute de quoi la population pourrait refuser de répondre au questionnaire, sans égard aux conséquences, ou fournira des réponses fictives et compromettra les données. Les gouvernements qui se sont succédés se sont montrés conscients qu'une garantie de confidentialité en contrepartie de renseignements personnels constituait un échange de bons procédés, et ont assumé leurs responsabilités à cet égard. De là l'impossibilité d'avoir accès aux données des recensements.

Cette mesure n'est certainement pas sans précédent. L'Australie, un pays ayant la même histoire et un intérêt aussi fervent que le nôtre pour la recherche généalogique, détruit ses formulaires de recensement une fois remplis pour protéger non seulement la vie privée des citoyens et des citoyennes, mais aussi son Bureau du recensement des tentatives d'autres organismes d'utiliser les données des recensements à d'autres fins.

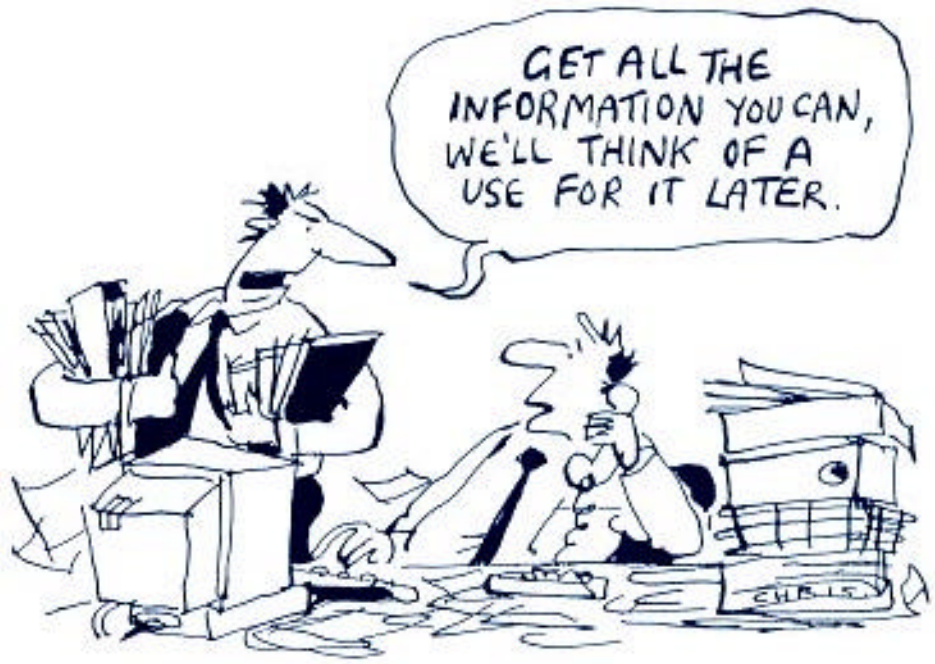
Malheureusement, l'exercice de pressions intenses semble donner des résultats au Canada. Notre ministre de l'Industrie a en effet demandé à Statistique Canada d'élaborer des options de modifications législatives afin de permettre l'accès aux données des recensements. Selon Statistique Canada, deux possibilités s'offrent. La première serait de modifier la *Loi sur la statistique* afin de permettre l'accès aux données des recensements de 2001 et des années subséquentes. La seconde consisterait en la modification rétroactive de cette même loi afin d'en annuler les dispositions régissant le caractère confidentiel des données des recensements depuis 1911.

Ni l'une ni l'autre de ces options ne sont attirantes. La première, en effet, risque de compromettre le processus de recensement si un nombre considérable de Canadiens et de Canadiennes s'y opposent. La seconde briserait la promesse que le Parlement a faite aux Canadiens et aux Canadiennes en 1911 et lors de chacun des recensements suivants, démontrant ainsi à la population la fragilité des promesses gouvernementales

devant les efforts d'un groupe de pression organisé. Cela serait aussi indésirable que l'intrusion dans la vie privée des citoyens et des citoyennes, et le Commissaire à la protection de la vie privée ne peut donc y souscrire.

Et maintenant, parlons un peu de votre sécurité financière…

S'il nous fallait une indication de la frustration et de la résistance croissantes des Canadiens et des Canadiennes devant les sondages du gouvernement, "l'Enquête sur la sécurité financière" menée par Statistique Canada serait un bon exemple.



Rassemble tous les renseignements que tu peux : on leur trouvera bien une utilité plus tard.

Ce sondage a de nouveau provoqué une controverse, dont la déclaration publique d'un commissaire provincial à la protection de la vie privée qui a indiqué qu'il refuserait d'y participer s'il était sollicité. Plusieurs des préoccupations soulevées au sujet du sondage sont analogues à celles qu'a abordées le Commissariat lorsqu'il s'est penché sur d'autres sondages tel celui sur les dépenses des familles dont traitait le rapport annuel de 1997-1998 : l'indiscrétion des questions, la sécurité du processus de collecte de l'information et toute communication possible des données recueillies.

Le sujet abordé, à savoir les finances, est toujours délicat, et la profondeur des questions du sondage dépasse le seuil de tolérance de certains. Le questionnaire de 68 pages jette un regard exhaustif sur les finances des ménages et est rempli lors d'entrevues individuelles auprès de quelque 21 000 ménages. Son but déclaré est de déterminer comment les Canadiens et les Canadiennes s'en tirent financièrement.

Pour répondre à cette grande question, le sondage recueille des renseignements personnels reliés à chaque membre du ménage. Les questions vont de la composition de la famille (niveau d'instruction, situation et expérience sur le marché du travail, déficiences physiques et intellectuelles) jusqu'à des détails très poussés sur les dépenses, l'épargne, les éléments d'actif, les régimes de retraite et la gestion des finances personnelles. Parmi les questions controversées, mentionnons celles qui demandent si le répondant a mis fin les 18 derniers mois à une relation avec une personne faisant auparavant partie du ménage, les raisons de la rupture, si les membres du ménage sont syndiqués, et les numéros d'enregistrement des régimes de pension. Statistique Canada demande également l'autorisation d'examiner les dossiers personnels de l'impôt sur le revenu et du Régime de pensions du Canada (ou Régime des rentes du Québec) des répondants.

Deux préoccupations sont cependant nouvelles : une déclaration figurant dans la trousse des sondeurs alléguant que les commissaires fédéral et provinciaux à la protection de la vie privée aient été consultés au sujet du sondage, et le peu de visibilité donné au caractère volontaire de ce dernier. La consultation auprès du Commissariat s'est limitée à un appel téléphonique annonçant l'intention de Statistique Canada de mener ce sondage. Une réunion a par la suite eu lieu deux semaines avant le début du sondage afin de "réviser" la documentation : en fait, il s'agissait là d'une pure formalité, car tous les documents étaient déjà imprimés et prêts à être distribués.

Le personnel du Commissariat a souligné la nécessité de clarifier auprès des répondants le processus et les options. Cela voulait dire qu'il fallait expliquer aux répondants que leur participation au sondage n'était pas obligatoire, qu'ils pouvaient remplir le questionnaire eux-mêmes (au lieu de le faire en présence du sondeur) et que les membres d'un ménage donné pouvaient avoir leur propre formulaire de sondage si nécessaire (les formulaires individuels sont importants dans les ménages constitués de personnes sans lien de parenté). Notre personnel a aussi contesté le fait que soient conservés les questionnaires identifiant leurs répondants, réitérant ainsi la position du

Commissariat voulant que la destruction de tout identifiant personnel soit une juste compensation pour la collecte de données très délicates.

Statistique Canada a indiqué que les sondeurs avaient expressément reçu instruction de mentionner que la participation au sondage était facultative. Statistique Canada a également accepté de prendre en considération les autres commentaires du Commissariat. Après la réunion, le Commissariat a lu tous les documents du sondage, et vu que la lettre de présentation ne mentionnait pas le caractère facultatif de leur participation. De plus, la brochure d'accompagnement était aussi plutôt vague. Les documents d'information des sondeurs étaient beaucoup plus clairs, et le personnel du Commissariat a proposé que des passages de ces documents soient incorporés dans la brochure destinée aux répondants. Mais il était déjà beaucoup trop tard pour cela. Quoi qu'il en soit, Statistique Canada a convenu de modifier la lettre pour faire ressortir le caractère facultatif de la participation, ce qui était le mieux qui ait pu être fait si près de la fin du processus.

Mais peu après le déploiement des sondeurs sur le terrain, il s'est avéré que la lettre n'avait pas été modifiée. Sommés de s'expliquer, les responsables de Statistique Canada ont indiqué que les directeurs régionaux pouvaient choisir la formulation de la lettre destinée aux répondants de leur région. Au moins deux d'entre eux avaient décidé que le fait de préciser que la participation au sondage était facultative aurait fait diminuer le nombre de répondants, et ont donc supprimé la mention en question.

Les citoyens doivent être informés des raisons pour lesquelles des renseignements personnels sont recueillis à leur sujet et de la façon dont ceux-ci seront utilisés et communiqués. Chaque personne doit aussi savoir si elle est légalement tenue de fournir ces renseignements. Ce sont là les principes fondamentaux de la *Loi sur la protection des renseignements personnels*, et non de simples droits facultatifs que des fonctionnaires peuvent arbitrairement décider d'ignorer lorsqu'ils ne font pas leur affaire. Le Commissaire mène actuellement enquête au sujet des plaintes déposées suite au sondage.

Sur la Colline

Les projets de loi ou de programmes gouvernementaux paraissent souvent simples et souhaitables à première vue. Qui songerait à s'opposer à la constitution d'un registre national de donneurs d'organes ou à l'amélioration du processus de dédouanement anticipé aux aéroports ou de détection du blanchiment d'argent ? L'intention est généralement louable; ce n'est que lorsque des détails commencent à émerger que les problèmes se remarquent. Plusieurs cas se sont présentés cette année.

La *Loi sur le recyclage des produits de la criminalité*

Au mois de mai 1998, le solliciteur général a publié un document de consultation sur les modifications législatives à apporter pour améliorer les capacités d'enquête policière en matière de blanchiment d'argent. Les propositions portaient notamment sur l'obligation pour les institutions financières de signaler les transactions suspectes, sur de nouvelles mesures d'application de la loi, sur la création de nouvelles infractions et sur la constitution d'un nouvel organisme fédéral pour recueillir et gérer l'information.

Toute disposition législative obligeant une institution financière à déclarer certaines transactions d'un de ses clients à un organisme gouvernemental porte automatiquement atteinte à la vie privée du client. Le défi consiste à permettre la détection des crimes financiers sans renoncer aux droits individuels. Le Commissariat a donc fait part de ses réserves dans une lettre adressée au solliciteur général. Celles-ci portent sur la conformité à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*, sur la définition de « transaction suspecte », sur le danger que l'obligation de déclarer ce type de transaction compromette le secret professionnel bancaire et suscite un climat de délation, ainsi que sur la structure et le mandat du nouvel organisme fédéral.

En février 1999, le ministère a rendu public son résumé des consultations avant de déposer, le 1er mai, son projet de loi C-81. Peu avant son congé estival, le Parlement a adopté ce dernier en tenant compte de certaines de nos préoccupations. Afin de sensibiliser le public, les décideurs et le législateur, nous répétons ici nos réserves, assorties des nouvelles dispositions législatives.

Conformité à la Charte

Nos réserves : Le fait d'obliger une institution assurant des services financiers (telle une banque, un courtier en investissements ou une compagnie d'assurance) de recueillir sans mandat préalable des renseignements confidentiels sur sa clientèle pour le compte des forces de l'ordre pourrait contrevenir aux dispositions de la Charte assurant une protection contre les « perquisitions ou saisies abusives ».

La nouvelle loi : Le solliciteur général partageait certaines de nos préoccupations et a donc obligé les forces de l'ordre à obtenir un mandat avant de demander au nouvel organisme fédéral de leur fournir tout renseignement **supplémentaire** (notre emphase). Bien que cette disposition apporte un certain contrôle indépendant dans le processus, elle ne résout cependant pas l'atteinte à la Charte que représente la collecte initiale de tels renseignements par l'institution assurant des services financiers ou par le nouvel organisme fédéral.

Conformité à la *Loi sur la protection des renseignements personnels*

Nos réserves : Cette loi exige que les organismes recueillant des renseignements personnels indiquent aux intéressés pourquoi ils le font et à quoi ces renseignements serviront. Il n'est permis de déroger à cette obligation que lorsqu'elle compromettrait l'exactitude des renseignements ou causerait préjudice à leur utilisation ultérieure. Le projet de règlement ne traite nullement du droit des personnes visées d'être informées. L'interdiction faite aux institutions assurant des services financiers d'informer leurs clients qu'elles doivent déclarer certaines transactions peut aider la détection de criminels sans cervelle, mais il est peut probable que les blanchisseurs d'argent aguerris d'y laisseront prendre. La pratique générale de l'avis public est un instrument utile de sensibilisation de la population.

La nouvelle loi : Le nouvel organisme fédéral est spécifiquement assujetti aux dispositions de la *Loi sur la protection des renseignements personnels*, bien que cela ne satisfasse pas de prime abord l'obligation du gouvernement d'informer dès le départ toute personne visée des raisons d'une collecte de ses renseignements financiers et des usages qui en seront faits. En effet, la collecte sera effectuée pour le compte du nouvel organisme fédéral par des entreprises privées échappant quant à elles aux obligations de la *Loi sur la protection des renseignements personnels*. Ce scénario ne permettra donc à toute personne visée de découvrir la divulgation de ses renseignements personnels au nouvel organisme fédéral qu'en demandant à ce dernier de lui remettre copie de ses renseignements.

Définition de « transaction suspecte »

Nos réserves : Il n'était pas évident que le montant de 10 000 $ proposé dans le document aurait suffi à rappeler à l'institution assurant des services financiers son obligation de déclarer la transaction, pas plus que ne l'aurait été tout indicateur supplémentaire, seul ou en combinaison, dit « suspect ». Le danger résidait dans le fait que l'institution s'en tiendrait au seul critère monétaire pour éviter d'avoir à poser un jugement (donc peut-être d'engager sa responsabilité), entraînant ainsi la déclaration possible d'un nombre considérable de transactions tout à fait régulières. Nous avons suggéré que la nouvelle loi prévoie une combinaison d'autres éléments de preuve s'ajoutant au critère monétaire. Quels que soient les indicateurs, ils devraient ressortir clairement de la transaction et des circonstances pertinentes immédiates. Ils ne devraient pas obliger l'institution à scruter en profondeur les affaires financières d'un client ou de tout tiers associé pour déterminer si la transaction est réellement « suspecte ».

La nouvelle loi : Cette dernière stipule clairement que le critère monétaire ne devrait pas être le seul qui soit déterminant. Toute institution assurant des services financiers doit obtenir des renseignements supplémentaires (énoncés dans le règlement) avant de décider qu'une transaction est suffisamment « suspecte » pour en faire rapport. Il s'agit là d'une grande amélioration, mais le Commissaire préférerait un débat public sur la question à l'élaboration quasi secrète de règlements.

Secret professionnel

Nos réserves : L'application des exigences de déclaration aux personnes qui se livrent à l'exploitation d'une entreprise, à l'exercice d'une profession ou à une activité qui leur permet de recevoir de l'argent comptant à verser ou à transférer à une tierce partie (tel un avocat ou un comptable) aurait pu enfreindre les exigences du *common law* en matière de secret professionnel.

La nouvelle loi : Cette dernière dispense désormais les avocats de toute obligation de rapport qui contreviendrait à leur devoir de respecter le secret professionnel.

Nouvel organisme fédéral

Nos réserves : L'organisme aura la tâche d'analyser les renseignements qu'il recevra des institutions et des personnes physiques tenues en vertu de la loi de faire des déclarations. Il recueillera également des renseignements auprès

de sources publiques, de services de police d'autres pays, d'informateurs et du Centre canadien d'information de la police. Il est à signaler que tous ces renseignements seront recueillis sans mandat. Toutefois, le statut précis dont jouira l'organisme n'est pas clair. Il semble que, sans être un organisme d'application de la loi ni un organisme d'enquête, il ait à exercer jusqu'à un certain point ces deux types de fonctions. La question de ce statut revêt une importance capitale parce que l'application de la *Loi sur la protection des renseignements personnels* aux renseignements qu'il recueillera ou détiendra en dépend. Les personnes touchées auront-elles le droit de consulter et de corriger ces renseignements ou ce droit leur sera-t-il refusé parce que les renseignements auront été obtenus "au cours d'une enquête licite" ? La collecte, l'utilisation et la divulgation de renseignements personnels par l'organisme sera-t-elle assujettie à des restrictions prévues par la loi ? Les personnes touchées seront-elles informées ? Les opérations de l'organisme feront-elles l'objet d'une surveillance indépendante ? Aucune de ces questions n'est traitée dans le document de consultation.

La nouvelle loi : Les modifications apportées n'ont pas clarifié le statut du nouvel organisme, dont on ignore toujours s'il est d'application de la loi ou d'enquête. Il est absolument impératif de répondre à cette question car en dépend la possibilité que le nouvel organisme invoque les dispositions de la *Loi sur la protection des renseignements personnels* lui permettant de recueillir des renseignements sans le consentement et à l'insu des personnes concernées, et de systématiquement refuser de les leur divulguer.

Nos réserves : Une fois que le nouvel organisme aura recueilli et analysé une grande quantité de renseignements lui permettant de conclure à la nature « suspecte » d'une transaction, son personnel pourra prévenir les forces de l'ordre. Le nouvel organisme ayant recueilli ces renseignements sans mandat, il devrait limiter la quantité de renseignements communiqués aux forces de l'ordre, tout renseignement supplémentaire ne pouvant être obtenu que sur présentation d'un mandat au nouvel organisme.

La nouvelle loi : Les renseignements que le nouvel organisme pourra initialement communiquer aux forces de l'ordre se limitent au nom de l'individu visé, au nom de l'institution assurant des services financiers, au montant de la transaction et à sa nature (comptant, bons d'épargne, actions, etc.). Tout renseignement supplémentaire ne pourra être obtenu que par le biais d'un mandat précisant ce que le nouvel organisme doit fournir.

Nos réserves : Il demeure que le nouvel organisme, du simple fait de qualifier une transaction de « suspecte », fournit aux forces de l'ordre des

motifs suffisants d'obtenir un mandat contre son personnel, ce qui pourrait mener à la délivrance systématique de tels mandats par suite des avis du nouvel organisme.

La nouvelle loi : Il demeure incertain que le simple avis du nouvel organisme constitue en soi un « motif raisonnable » d'obtenir un mandat, ou si les tribunaux auront besoin de plus de renseignements avant d'émettre un mandat.

Un Registre de dons d'organes

Les propositions relatives à la création d'un nouveau registre de dons d'organes constituent un autre exemple de bonnes intentions qui ont besoin d'être approfondies. Le Comité permanent de la Chambre des communes sur la santé a étudié des moyens d'élever le faible taux national de dons d'organes. La création d'un registre national de donneurs figurait parmi les propositions initiales. Le comité a demandé l'avis du Commissaire sur les points qu'il fallait examiner en matière de protection de renseignements personnels avant de recommander l'établissement d'un tel registre.

Les avantages d'un registre de donneurs sont manifestes, pourtant il faut de solides justifications pour recueillir des renseignements pouvant être très délicats et les conserver dans un registre central. N'ayant pas les ressources nécessaires pour effectuer un examen approfondi, le Commissaire n'a pu formuler que des observations préliminaires. Il a recommandé au comité de se pencher sur plusieurs questions.

Existe-t-il de solides justifications à la collecte et à l'entreposage central des données ?
Le Commissariat entend souvent l'argument voulant que la collecte, l'utilisation ou la divulgation de renseignements personnels concernant des citoyens canadiens servira l'intérêt public, facilitera des activités gouvernementales ou aidera à l'application des lois. Nous hésitons de plus en plus à accepter d'emblée de telles déclarations compte tenu, en particulier, de l'absence d'éléments de preuve valables et de l'intrusion qui accompagne par définition la collecte.

Quels renseignements entreraient dans la base de données proposée ?
S'agirait-il simplement de l'acquiescement à devenir un donneur, accompagné des détails nécessaires pour communiquer avec la personne (adresse et numéro de téléphone), ou bien la base de données comprendrait-elle des renseignements médicaux pertinents comme le groupe sanguin et la

constitution génétique ? S'il devait y avoir inclusion de renseignements médicaux, quelles mesures de sécurité seraient mises en place pour protéger les renseignements de tout accès ou de toute divulgation non voulue ?

L'information servirait-elle à d'autres fins que celle du jumelage des organes et des tissus ?
Au Canada, les bases de données posent un problème récurrent. Leur utilisation, une fois qu'elles ont été constituées pour une fin donnée, tend à dépasser les usages qui avaient été prévus au moment de la collecte initiale. En règle générale, il faudrait interdire toute utilisation secondaire des renseignements à moins que les personnes concernées ne l'aient expressément autorisée en toute connaissance de cause. Une base de données visant à faciliter les dons d'organes ne devrait servir à aucun autre programme gouvernemental, comme l'application de certaines lois.

À qui les renseignements seraient-ils divulgués ?
Si la base de données vise à faciliter le don d'organes, les renseignements qu'elle renferme ne devraient pas être divulgués pour d'autres fins à moins que les personnes concernées n'y aient expressément consenti. Il est arrivé trop souvent que des renseignements recueillis et utilisés dans l'intérêt public aient ensuite été communiqués à des fins beaucoup moins acceptables.

Convient-il de créer le registre en utilisant les formulaires de déclaration de revenus ?
Le gouvernement a utilisé cette méthode pour recueillir des adresses pour sa liste permanente d'électeurs. Bien que cela puisse se justifier du fait que le maintien d'une liste à jour et exacte soit essentiel à une démocratie saine et fonctionnelle, un registre de dons d'organes pourrait ne pas satisfaire à un critère analogue de nécessité publique. Combien d'autres causes louables pourraient se réclamer de la même utilité, et quelles en seraient les répercussions sur les formulaires de déclaration de revenu ?

Le Commissaire a proposé de discuter de ces réserves devant le comité. Toutefois, ce dernier a suivi une démarche prudente dans son rapport (rendu public en avril 1999), concluant que la création de ce registre ne constituerait pas l'utilisation la plus efficiente de ressources. Le comité a recommandé la constitution de listes nationales de personnes en attente d'organes "pleins" (tel le cœur), de donneurs effectifs et de donneurs potentiels à l'hôpital. Il a également proposé qu'une base de données nationale suive les résultats des dons d'organes au moyen du Registre canadien des insuffisances et des transplantations d'organes. Toutes les listes proposées sont plus axées sur les personnes et sur les processus médicaux en cause et sont de loin préférables à une base de données nationale générale.

Les conclusions et les recommandations du comité nous rappellent avec pertinence de songer à signer notre carte de don d'organes.

La commodité du pré-contrôle aux douanes américaines

Les efforts déployés en vue d'accélérer les voyages en avion entre le Canada et les États-Unis (et d'accroître l'attrait du Canada en tant que porte d'entrée des déplacements internationaux vers l'Amérique du Nord) ont amené le gouvernement à déposer un projet de loi autorisant les responsables américains en poste dans les principaux aéroports canadiens à dédouaner les voyageurs voulant entrer aux É.-U.

Le pré-contrôle permettrait aux voyageurs canadiens de s'acquitter des formalités dès le début de leur voyage, puis de s'envoler vers n'importe quelle destination américaine, au lieu des seules destinations dotées de services des douanes et de l'immigration. Les voyageurs internationaux pourraient réduire la durée de leurs envolées en transitant par le Canada, sans pour autant avoir à obtenir de visa canadien ou à passer par les douanes canadiennes lorsqu'ils s'en vont aux É.-U. Cela devrait inciter davantage les voyageurs d'autres pays à utiliser un transporteur canadien.

Le projet de loi S-22, la *Loi sur le pré-contrôle*, officialise un accord intervenu en 1974 entre le Canada et les É.-U. et qui permet aux agents américains des douanes et de l'immigration de dédouaner les visiteurs canadiens ou les voyageurs internationaux en transit dans les aéroports canadiens. Le gouvernement canadien ne promulguera pas le projet de loi tant que l'accord original n'aura pas été modifié pour assurer la réciprocité. La procédure présente certes des avantages indéniables, mais aussi quelques imperfections.

Le projet de loi permettrait aux autorités américaines de filtrer les voyageurs en fonction des règlements sur les douanes, l'immigration, la santé publique et les aliments. Il aurait aussi pour effet d'élargir les pouvoirs qu'elles ont déjà du simple refus de l'entrée aux É.-U., à la fouille (sommaire), à la saisie de biens et à l'impositions d'amendes. Les agents des douanes américains ne pourraient pas procéder à des arrestations, mais seulement remettre aux autorités canadiennes les personnes jugées suspectes. Même si les pouvoirs en question ne sont pas nouveaux, puisque les responsables des douanes dédouanent déjà les voyageurs en vertu de l'accord de 1974, c'est la première fois qu'ils sont énoncés dans une loi. Dans les faits, le projet de loi accorde aux responsables d'une puissance étrangère le droit de réunir de l'information en sol canadien. Le projet suscite également des inquiétudes considérables

quant à l'application extraterritoriale de dispositions législatives américaines et à la protection offerte par les lois canadiennes en sol canadien.

La *Loi sur la protection des renseignements personnels* est l'une de ces lois. Toutes les procédures frontalières ont pour effet de réunir de l'information. Le fait d'entrer dans un pays étranger est un privilège; le respect des conditions d'entrée du pays en question est donc essentiel. Mais l'information est généralement recueillie dans le pays hôte et régie par les lois de celui-ci. Étant donné que le projet de loi S-22 fait passer une partie de la collecte de données au Canada, est-ce que les règles canadiennes relatives à la protection de la vie privée s'appliqueront?

Le ministère des Affaires étrangères nous assure que toutes les utilisations de renseignements personnels seront conformes aux dispositions législatives et aux politiques canadiennes sur la protection de la vie privée. Le projet de loi comporte des références précises à la *Charte canadienne des droits et libertés* et à la *Loi canadienne sur les droits de la personne*. Et il est manifeste que, lorsqu'une personne est détenue et remise aux autorités canadiennes, les dispositions législatives canadiennes sur la protection de la vie privée s'appliqueront. Mais ces affirmations entraînent plusieurs questions : les particuliers auront-ils le droit de consulter et, s'il y a lieu, de corriger l'information réunie par les autorités américaines ? Pourront-ils en contester la collecte, l'utilisation et la communication ? Et, dans l'affirmative, auprès de qui les passagers pourraient-ils demander que soit revue la façon dont les responsables américains traitent les renseignements personnels qui ont été réunis en sol canadien en vue de l'application d'une loi américaine ?

Pour les passagers en transit au Canada, les agents des douanes américains réuniraient aussi des renseignements ou des profils de nature "comportementale". Ces données comprendraient la ville où le voyage a commencé et toute autre ville visitée, les interruptions durant le voyage, le moment où le billet a été acheté, le mode de paiement et le nom de la personne qui a payé le billet, le nom de l'agent de voyage, les préférences en matière de siège et de repas et tout numéro de téléphone qui aurait été donné. La compagnie aérienne internationale communiquerait les données aux autorités américaines en poste au Canada à des fins de comparaison avec le profil de voyageurs suspects. Les personnes répondant aux profils établis pourraient être la cible d'un examen secondaire et se voir refuser l'entrée aux É.-U. Les dispositions législatives américaines ne prévoient pas la révision d'une telle décision.

Les responsables des douanes canadiens ne sont pas autorisés à recourir à l'établissement de profils pour la prise de décisions d'ordre administratif au sujet des voyageurs. En autorisant cette pratique en sol canadien, l'accord semble paver la voie à l'utilisation de cette technique par les douanes canadiennes, une technique que le Commissaire à la protection de la vie privée trouve troublante et à laquelle la population a jusqu'ici su résister. Est-ce là l'intention du Parlement ?

Pour tout dire, il est difficile d'accepter l'assertion selon laquelle le projet de loi reflète les dispositions législatives et les pratiques canadiennes en matière de protection de la vie privée. Il est ironique que le projet de loi reconnaisse la primauté de la *Loi canadienne sur les droits de la personne*, la première à établir les droits des Canadiens et des Canadiennes au chapitre de la protection de la vie privée, mais pas la primauté de la *Loi sur la protection des renseignements personnels*, plus récente et plus complète.

Le Sénat réclame des tests de dépistage antidrogue

En juin 1998, le Sénat mettait sur pied un comité spécial chargé d'examiner, afin de présenter des recommandations, l'état de la sécurité des transports au Canada. Dans son rapport provisoire de janvier 1999, le Comité sénatorial spécial sur la sécurité des transports exhortait le gouvernement à permettre les tests obligatoires de dépistage d'usage de drogues et d'alcool dans l'industrie des transports, reflétant ainsi les dispositions législatives américaines actuelles en la matière.

Nul ne peut s'opposer à des mesures visant à accroître la sécurité des transports au Canada et le comité a fait plusieurs recommandations judicieuses à cette fin. Nous sommes toutefois troublés de voir que le comité accepte aussi facilement l'idée que les tests antidrogue sont nécessaires et accroîtront la sécurité dans les transports.

Le Commissariat s'est penché à plusieurs reprises sur la question des tests antidrogue. Et chaque fois, la même question s'est posée : les tests aléatoires généralisés sont-ils la solution ? Le test antidrogue est en soi envahissant, mais ne peut même pas révéler si la personne qui le subit a les facultés affaiblies. De plus, l'information qu'il produit est non seulement de nature délicate mais aussi sujette à des abus. Vu leur caractère envahissant, les tests antidrogue ne devraient être imposés par l'État que lorsque des preuves irréfutables attestent de leur nécessité.

Il n'existe guère de preuves à l'effet que bon nombre des types de tests antidrogue auxquels souscrivent avec tant d'enthousiasme les gouvernements et le secteur privé et qui sont si habilement commercialisés par les entreprises spécialisées accroissent réellement la sécurité au travail. Dans la majorité des cas, les tests antidrogue ont pour seul effet notable une atteinte sérieuse au droit fondamental au respect de la vie privée. Trop souvent, les tests antidrogue ne font que dépouiller les gens de leur dignité et de leurs droits constitutionnels sur la foi d'affirmations douteuses relatives à leur efficacité.

Donc, le vrai avantage du test d'urine, c'est d'humilier nos employés?

Dans une étude détaillée parue en 1990 et intitulée *Le dépistage antidrogue et la vie privée*, le Commissaire a fait plusieurs recommandations au sujet des programmes généralisés de tests antidrogue. Parmi celles-ci figurait la recommandation voulant qu'on puisse être justifié de recueillir des renseignements personnels par des tests aléatoires obligatoires de membres d'un groupe en raison du comportement du groupe dans son ensemble uniquement si les conditions suivantes sont réunies :

- Il y a des motifs raisonnables de croire qu'il se fait un usage substantiel de drogues au sein du groupe ou que le groupe fait montre de facultés affaiblies;

- L'usage de drogues ou l'affaiblissement des facultés menace sérieusement la sécurité publique ou de membres du groupe;
- La conduite de certains des membres du groupe ne peut être surveillée que par le biais de tels tests;
- Il y a des motifs raisonnables de croire que les tests antidrogue peuvent substantiellement réduire toute menace posée à la sécurité; et
- Il n'existe aucune autre façon pratique moins envahissante (tels des examens médicaux périodiques, une sensibilisation et/ou un suivi thérapeutique) de substantiellement réduire une telle menace.

Rien dans les années qui ont suivi la publication de notre étude n'a modifié notre opinion selon laquelle l'administration généralisée de tels tests est injustifiée. Le Commissaire a demandé l'autorisation de comparaître devant les membres du comité afin d'exprimer ses préoccupations.

La *Loi sur le système correctionnel et la mise en liberté sous condition*

Le Comité permanent de la justice et des droits de la personne est en train de procéder à l'examen quinquennal de la *Loi sur le système correctionnel et la mise en liberté sous condition* (la *LSCMLC).* Au début de 1998, le solliciteur général du Canada a requis la contribution du public dans un document de consultation intitulé *Pour une société juste, paisible et sûre*. Les détenus conservant la majorité de leurs droits, il est essentiel d'appliquer les dispositions de la *Loi sur la protection des renseignements personnels* (la *LPRP*) à toute modification envisagée à la *LSCMLC*. Il ne s'agit pas ici d'une question de choix mais bien d'une complémentarité obligée.

Le Commissaire à la vie privée a concentré ses observations sur quatre questions.

Le rapport entre la *LSCMLC* et la *LPRP* : Bien que la *LSCMLC* garantisse aux détenus à peu près les mêmes droits d'accès à l'information que la *LPRP*, elle ne prévoit pas d'examen indépendant des plaintes. Un détenu ayant obtenu des renseignements personnels en vertu de cette première loi pourrait vouloir porter plainte auprès du Commissaire à l'information si ces renseignements sont inexacts. Services correctionnels Canada (SCC) et la Commission nationale des libérations conditionnelles (CNLC) prétendent cependant que les détenus n'ont le droit de faire corriger

que les renseignements obtenus en vertu de la *LPRP*. Les détenus se voient donc dans l'obligation de présenter en bonne et due forme une demande de communication de renseignements personnels qui sont déjà en leur possession. Bel exemple de bureaucratie ! Le Parlement devrait modifier la *LSCMLC* afin que tout renseignement obtenu en application de cette loi soit également réputé avoir été fourni en vertu de la *LPRP*.

Tests d'urine : Le mémoire réitère les observations formulées dans notre étude de 1992. Le dépistage de drogues constitue une grave intrusion dans la vie privée, et même si les détenus s'attendent à moins de respect à l'égard de leur vie privée que le reste de la population, il convient de ne pas les priver au-delà du strict nécessaire d'un droit de la personne qui est fondamental. Il ne faudrait donc pas recourir aux tests de dépistage sauf s'il peut être établi que ceux-ci permettent de réduire à la fois la consommation de drogues et l'incidence de la violence dans les établissements.

Le solliciteur général a soutenu en 1992 que tel serait effectivement le cas, ce que le dernier document de consultation ne corrobore pas. Au contraire, d'après certains indices, les détenus passeraient à des drogues plus dures dont la consommation est plus difficile à déceler. Rien ne permet donc de croire que l'augmentation significative du nombre de tests de dépistage dans les établissements donne les résultats attendus. À ce que l'on nous a dit, le solliciteur général compte se pencher sur la question. Nous attendons les résultats avec impatience. Il est primordial que le dépistage de la consommation de drogues ne pousse pas à une modification des habitudes de consommation propre à favoriser la propagation du VIH, de l'hépatite et d'autres infections transmissibles par le sang.

Information relative aux contrevenants : Le document de consultation indique que l'échange d'information sur les détenus entre SCC et la CNLC a été quelque peu problématique. Nous avons été rassurés d'apprendre que la *LPRP* n'était pas en cause. Celle-ci renferme, aussi bien que la *LSCMLC*, des dispositions qui permettent à SCC comme à la CNLC de mettre en commun l'information dont les deux organismes ont besoin pour s'acquitter de leurs responsabilités.

La notion de justice intégrée a fait l'objet d'une mise en garde. Toute partage supplémentaire de renseignements personnels entre les différents intervenants du système judiciaire doit respecter les dispositions pertinentes en matière de protection de la vie privée, et nous avons demandé instamment à ce que les commissaires fédéral, provinciaux et territoriaux à la vie privée soient consultés le plus rapidement possible à ce sujet.

Le Registre des décisions de la CNLC : Il arrive souvent qu'un bon compromis permette de régler un conflit apparent entre le droit du public à apprendre certains détails au sujet d'une personne donnée et le droit de cette même personne au respect de sa vie privée. Le Registre des décisions de la CNLC pourrait éventuellement en devenir un bon exemple.

Plusieurs plaintes déposées par des détenus souhaitant une libération conditionnelle mentionnaient les nombreux détails fournis par la CNLC dans ses "feuilles de décision", que toute personne intéressée peut consulter dans le Registre des décisions. Nos enquêtes à l'égard de ces plaintes ont révélé que ces "feuilles" contiennent dans certains cas des détails considérables de nature psychologique et se rapportant au traitement et même, dans un cas, de l'information financière. Le Commissaire à la protection de la vie privée a jugé que certains des renseignements communiqués étaient superflus et que les plaintes étaient fondées. Il en a avisé la CNLC par écrit.

Depuis lors, la CNLC a tenu des séances de formation à l'intention de ses membres (qui rédigent les décisions) et de ses employés portant sur les liens entre sa loi habilitante et la *Loi sur la protection des renseignements personnels*. La première exige la communication au public, mais la seconde donne aux candidats à la libération conditionnelle accès à leurs propres renseignements personnels tout en protégeant ceux-ci contre la communication à des tiers.

Cette mesure s'est traduite par des décisions généralement plus courtes et une plus grande mise en relief des détails liés strictement à la décision.

Nous comprenons, certes, que la CNLC doive rendre compte de ses décisions quant à la remise en liberté de détenus avant la fin de leur sentence. Et nous sommes conscients des améliorations qui sont intervenues, attestées par la prestation d'une formation continue. Il reste toutefois que la CNLC vise deux objectifs incompatibles : expliquer la décision de la CNLC au candidat à la libération conditionnelle, et rendre des comptes au public.

Les "feuilles" de décision sont plus qu'une simple page résumant la décision et les facteurs qui sont intervenus dans la décision de la CNLC. Elles constituent la décision écrite de la CNLC qui a été prise à l'issue de l'audience, et c'est le document que reçoit le candidat. L'information, que doit connaître le candidat, peut comprendre des détails psychologiques ou de l'information sur le traitement suivi par le détenu, ou encore des renseignements sur les membres de la famille et d'autres tiers.

En fait, le Registre des décisions n'existe pas en tant que tel. Il n'y a pas de base de données contenant les décisions de la CNLC. Lorsqu'un membre du public demande à voir la feuille de décision, celle-ci est extraite du dossier du candidat. La feuille vise donc deux fins, soit fournir au candidat le plus possible de renseignements sur la décision de la CNLC tout en n'allant pas trop loin pour ce qui est de la communication de détails au public. Les intérêts dont il faut tenir compte ici sont trop contradictoires pour être conciliés en un seul document.

Le Commissaire a recommandé à la CNLC de créer un registre public qui soit réel et distinct et qui contienne de l'information sommaire sur les candidats à la libération conditionnelle et sur les décisions prises, ainsi qu'un résumé des raisons qui ont conduit à la décision. Voilà qui répondrait à l'obligation qu'a la CNLC de rendre des comptes au public. Puis les membres de la CNLC pourraient fournir aux candidats un document détaillé expliquant leurs décisions sans risquer la communication de renseignements superflus au public.

La CNLC a rejeté la recommandation, qui, comme plusieurs autres, se retrouve dans le mémoire que le Commissariat a présenté au solliciteur général concernant la révision de la *LSCMLC*, actuellement l'objet d'un examen par un comité parlementaire.

La *Loi sur l'identification par les empreintes génétiques*

Le Sénat a adopté la *Loi sur l'identification par les empreintes génétiques* en décembre 1998, sans modification, mais non sans réserves. En vertu de cette loi, le solliciteur général doit constituer une base de données nationale comprenant les profils d'identification génétique relevés sur les scènes d'actes criminels en prévision des enquêtes de la justice pénale. Élément encore plus important dans le contexte de la protection de la vie privée, la base de données comprendra tant les profils d'identification génétique que les échantillons d'ADN des personnes ayant été reconnues coupables d'infractions "désignées" (généralement des actes criminel avec violence). La base de données relèvera du Commissaire de la GRC.

La loi représente la deuxième phase de l'adoption de dispositions législatives relatives à l'utilisation des empreintes génétiques dans les enquêtes criminelles. La première phase, permettant la prise d'échantillons d'ADN par la force sur les suspects faisant l'objet d'un mandat, a été promulguée en 1995.

Le Commissaire à la protection de la vie privée a exprimé plusieurs réserves devant les comités permanents de la Chambre des communes et du Sénat chargés d'étudier le projet de loi, avec des résultats plus ou moins heureux.

Le Parlement a rejeté notre recommandation voulant que la loi ne permette pas la conservation, mais plutôt la simple analyse, des échantillons d'ADN recueillis sur des contrevenants reconnus coupables. Le risque inhérent à la conservation des échantillons réside dans la tentation que celle-ci offre aux gouvernements futurs d'autoriser d'autres tests à des fins n'ayant aucun rapport avec l'objet des échantillons.

En réponse à ses propres réserves, le Comité sénatorial des affaires juridiques et constitutionnelles a obtenu que le solliciteur général prenne plusieurs mesures, notamment :

- La mise sur pied d'un comité consultatif comprenant un représentant du Commissariat fédéral à la protection de la vie privée, chargé de superviser l'application de la loi et la gestion de la base de données d'empreintes génétiques. Le comité a exhorté le solliciteur général à inclure la nomination du comité dans les règlements d'application de la loi.

- La publication de ces règlements avant leur entrée en vigueur, pour donner au Sénat le temps de les examiner et de faire ses commentaires.

- La clarification, dans les règlements, de la notion de "profil d'identification génétique". Les règlements préciseront que l'établissement d'un profil d'identification génétique ne vise pas des raisons médicales, ce qui limitera l'utilisation, par la police, des profils génétiques pour l'identification de prévenus à des fins policières, et non pas pour la définition de caractéristiques médicales, physiques ou mentales. Cette clarification contribue à atténuer les préoccupations du comité sénatorial (et les nôtres) au sujet des dangers découlant de la conservation des échantillons.

- La possibilité d'inclure une disposition prévoyant l'examen quinquennal de la loi par le Parlement, étant donné la nature très délicate de l'information concernée et la rapidité de l'évolution technologique.

Au moment d'écrire ces lignes, nous croyons comprendre que le solliciteur général est en train d'élaborer un mandat pour le comité consultatif. Nous verrons à ce que le comité soit vraiment indépendant, et nous participerons à ses travaux dans toute la mesure que le permettent nos ressources.

Il est absolument essentiel de suivre de près les dispositions de notre droit criminel relatives aux empreintes génétiques. Des pressions considérables s'exercent déjà sur d'autres gouvernements pour que ceux-ci élargissent de beaucoup le nombre de personnes dont les empreintes génétiques pourraient être relevées à des fins d'enquête criminelle. Notre population subira certainement de telles pressions dans un proche avenir. À moins que tous n'y résistent, nos citoyens courent le risque, comme le gouvernement l'envisage sérieusement à l'heure actuelle en Grande-Bretagne, que chaque individu, qu'il soit innocent ou coupable, soit tenu de fournir ses empreintes génétiques aux forces de l'ordre au nom d'un soi-disant avancement de la répression de la criminalité et d'une renonciation certaine à ses droits à une vie privée.

Direction de l’Analyse et gestion des enjeux

La direction de l’Analyse et gestion des enjeux étudie les programmes et lois gouvernementaux, effectue de la recherche sur les questions de l'heure, et conseille le Commissaire à la protection de la vie privée en matières de politiques et de communications.

Un petit groupe de chefs de portefeuille sert de point de référence aux agences fédérales afin de résoudre toute question avant qu'elle ne mène à une plainte. Mise de l'avant au cours de l'année qui vient de s'écouler, cette approche proactive a remplacé les vérifications formelles et les suivis.

La direction emploie également quelques analystes de politiques et agents de recherche. Ces employés informent le Commissariat de toutes les nouveautés se rapportant à la vie privée, étudient les nouvelles lois et programmes gouvernementaux, et se penchent sur les développements au Canada et à l'étranger afin d'établir des positions sur des questions particulières et d'apporter au Commissaire les renseignements de fond dont ce dernier pourrait avoir besoin pour ses présentations au public.

Le personnel de la direction aide aussi à étudier certaines questions plus complexes ne relevant pas du mandat du Commissaire, et fournit aux agents de renseignements du Commissariat du matériel de référence sur certains sujets précis. Le personnel agit aussi comme point de contact pour les responsables étrangers de la protection de la vie privée s'intéressant à la situation canadienne, et collabore avec ses collègues des Enquêtes en leur dispensant de l'information et en obtenant des conseils d'experts selon les besoins.

C'est de cette direction qu'origine depuis toujours la majeure partie de la recherche et de l'expertise offertes au Commissaire en vue de ses communications au public. Cette année, la direction a assumé la responsabilité tant des communications ainsi que du suivi avec le Parlement, permettant ainsi au Commissaire de canaliser ses efforts et de mieux répondre aux nouveaux enjeux affectant la vie privée. Plus particulièrement, cette nouvelle polyvalence a permis d'aider le Commissaire à réagir à la poussée d'attention que le projet de loi C-54 a value au Commissariat. En fait, l'évolution de ce projet de loi a accaparé toutes les ressources que la direction avait de libres.

En plus de suivre la question de l'inforoute de la santé, la direction s'est aussi penchée sur les nouvelles lois et les questions reliées au NAS et traitées dans les pages précédentes. Son personnel a également suivi de près l'évolution de nombreuses autres questions, dont des enquêtes portant sur des agences gouvernementales, la politique fédérale de surveillance vidéo et le renouvellement du Centre canadien d'information de la police (CCIP).

Transfert de la Voie maritime du Saint-Laurent : 10 sur 10

La récente vague de privatisation semble s'être apaisée. Auparavant source d'inquiétude considérable puisque les clients et les employés y perdaient leurs droits en matière de protection de la vie privée, la privatisation ne figure plus au premier rang des dangers qui menacent cette dernière.

Deux éléments ont atténué les risques. Le premier devrait être l'adoption d'une loi qui s'applique au secteur privé de compétence fédérale. Presque tous les organismes qui ont été commercialisés œuvrent dans ce secteur et devraient pour cette raison tomber sous le coup de la nouvelle *Loi sur la protection des renseignements personnels et les documents électroniques*.

Le second élément est une compréhension et une conscience croissantes, chez les organismes privatisés, de la nécessité (et des avantages) d'un nettoyage en règle des dossiers sur leur personnel. Le fait de retirer des dossiers des renseignements inutiles et d'obtenir le consentement des employés au transfert des documents qui restent peut en effet s'avérer avantageux. Les employés participent à part entière au processus, et l'organisation peut souvent se débarrasser de tonnes de papier.

L'Administration de la Voie maritime du Saint-Laurent est l'un des derniers organismes à avoir été privatisé. Le transfert des dossiers personnels de l'Administration s'est fait de façon harmonieuse et ordonnée, et l'on peut voir pourquoi. Plusieurs mois avant le 1er novembre 1998, date du transfert, l'Administration s'était engagée à continuer à respecter les principes et les lignes directrices de la *Loi sur la protection des renseignements personnels*. Bien que la plus grande partie des renseignements sur les employés aient été conservés par les Ressources humaines de l'Administration, les cadres supérieurs avaient donné instruction aux superviseurs d'examiner leurs dossiers de travail pour voir s'il ne s'y trouverait aucun document de nature personnelle sur leurs employés. Les cadres supérieurs avaient même indiqué les grandes catégories de documents visés, les périodes de conservation applicables et si les documents devant être détruits ou envoyés aux Ressources humaines.

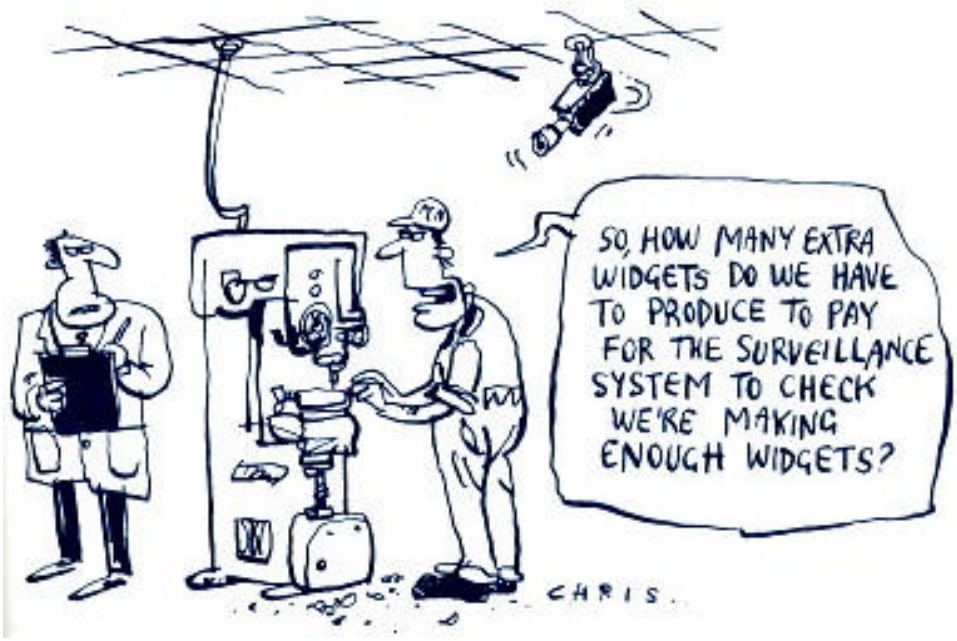
La direction avait ensuite écrit à tous les employés mutés au nouvel organisme privé pour leur expliquer l'information qui serait nécessaire à la poursuite de leurs salaires et avantages sociaux, ainsi qu'au respect des conventions collectives et des réclamations en découlant. La lettre énumérait ensuite les autres renseignements personnels détenus par l'Administration et demandait aux employés leur consentement au transfert de l'information. Les employés pouvaient consentir au transfert de la totalité ou d'une partie seulement des renseignements, voire d'aucun, sans conséquence défavorable sur leur emploi au sein du nouvel organisme. Les superviseurs avaient alors été informés des documents qui ne devaient pas être transférés, avant de signer une confirmation écrite de leur destruction.

Le processus, dans son entier, s'est avéré relativement indolore et a fait encore la preuve que les bonnes pratiques en matière de protection de la vie privée sont de bonnes pratiques en matière de gestion de l'information. Quel nouvel organisme ne voudrait-il pas bien faire les choses dans ce domaine et ce, dès le début?

Une plainte donne une politique sur la surveillance vidéo

Nous faisions état l'an dernier d'une plainte déposée par une employée, selon laquelle la Commission de l'immigration et du statut de réfugié (la CISR) avait installé une caméra dans le plafond au-dessus de son bureau parce qu'elle la soupçonnait de divulguer de l'information sur les audiences de la CISR. Le Commissaire à la protection de la vie privée avait conclu que les éléments de preuve recueillis par la CISR étaient si faibles que celle-ci aurait dû mener une enquête préliminaire approfondie avant de recourir à une surveillance aussi indiscrète. Troublé par le fait que la gestion ait eu recours aussi rapidement à une caméra vidéo cachée, le Commissaire a écrit au Conseil du Trésor pour l'exhorter à rédiger une politique gouvernementale sur la surveillance secrète des employés fédéraux.

En avril 1999, le Conseil du Trésor a émis un Avis de mise en œuvre de la politique sur la sécurité à tous les ministères dans le but de guider les responsables de la sécurité dans l'utilisation de caméras pendant les enquêtes. Évoquant les droits des particuliers à raisonnablement s'attendre au respect de leur vie privée qui sont prévus dans la *Charte canadienne des droits et libertés* et les droits conférés par la *Loi sur la protection des renseignements personnels*, l'Avis énonce toutes les conditions relatives à la surveillance, lesquelles sont fondées sur celles publiées dans notre rapport annuel de 1997-1998.



Hé ! combien de bébelles supplémentaires est-ce qu'on devra fabriquer pour payer la machine qui surveille si on fabrique assez de bébelles ?

D'après l'Avis, toute politique sur la surveillance vidéo secrète doit tenir compte des éléments suivants :

- Avant qu'une surveillance vidéo secrète ne soit envisagée comme moyen d'enquête, il faut qu'il existe des motifs raisonnables de soupçonner un employé d'inconduite grave, pouvant être de nature criminelle;
- Une surveillance vidéo secrète soulève évidemment plus de préoccupations quant à la vie privée qu'une surveillance vidéo avouée, et il ne faudrait envisager d'y recourir que lorsque toutes les autres mesures raisonnables, y compris des mesures qui n'ont pas le caractère d'une enquête, telles que le traitement thérapeutique, l'affichage d'avis en milieu de travail, les programmes d'éducation et une surveillance avouée, se sont avérées inefficaces ou sont susceptibles de s'avérer inefficaces;
- Il ne faut pas recourir à une surveillance vidéo secrète là où une personne peut raisonnablement s'attendre au respect de sa vie privée (par exemple, un bureau privé, des vestiaires ou un bureau fermé dans un environnement à aire ouverte). Si l'on estime que la présumée conduite devant faire l'objet de l'enquête est de nature criminelle, il faudrait alors

confier l'enquête à la police. Cette démarche exigera une révision judiciaire préalable, car la police devra d'abord obtenir un mandat pour effectuer une surveillance vidéo secrète dans un endroit où l'on peut raisonnablement s'attendre au respect de sa vie privée;

- Dans les endroits où les particuliers ne peuvent pas raisonnablement s'attendre au respect de leur vie privée (par exemple, un endroit accessible au public, un hall d'accueil), la décision d'effectuer une surveillance vidéo secrète doit être prise uniquement par un cadre supérieur, sur le conseil d'un agent de sécurité et des services juridiques du ministère; habituellement, les sous-ministres doivent être informés d'avance qu'une surveillance vidéo secrète sera effectuée;
- Dans la mesure du possible, une surveillance vidéo secrète ne devrait pas compromettre la vie privée de personnes autres que celle faisant l'objet de l'enquête;
- La surveillance ne devrait pas durer plus longtemps que cela est raisonnablement nécessaire pour les besoins de l'enquête;
- L'accès à la bande vidéo ou à toute information produite au moyen de la bande vidéo devrait être strictement limité aux personnes qui ont besoin de connaître les faits; la bande vidéo et l'information ne devraient pas être utilisées, par exemple, comme un moyen de surveiller le rendement général de l'employé. La bande vidéo et toute information recueillie pendant l'enquête sont visées par la *Loi sur la protection des renseignements personnels*, la *Loi sur l'accès à l'information* et la *Loi sur les Archives nationales du Canada*;
- À moins qu'il n'existe des raisons importantes de ne pas le faire, une personne ayant fait l'objet d'une surveillance vidéo secrète devrait en être informée après coup, en lui précisant les dates et le lieu de la surveillance et le motif de celle-ci.

Renouvellement du CCIP

Au mois d'avril 1999, le Solliciteur Général a annoncé que des fonds seraient alloués pour la modernisation et le renouvellement du Centre canadien d'information de la police (CCIP), le réseau informatique à la disposition des forces de l'ordre canadiennes. Le CCIP est une coopérative gérée par la Gendarmerie royale du Canada et dont sont membres les services de police

municipaux et provinciaux. D'autres organismes comme Douanes Canada et les Services correctionnels du Canada jouissent d'un accès restreint au réseau.

Les gestionnaires du CCIP appliquent un code rigoureux de protection de la vie privée au volume considérable de renseignements personnels que ce système contient et rend accessibles. Comme le renouvellement du système devra également porter sur les questions de protection de la vie privée, ces gestionnaires se sont adjoint un fonctionnaire expérimenté de notre Commissariat pour la durée du projet.

La bonne parole

Outre les comparutions du Commissaire devant les comités parlementaires sur les lois dont nous avons traité plus haut, celui-ci ainsi que son personnel ont pris la parole devant des auditoires allant des étudiants en droit de l'université Dalhousie à un groupe de chômeurs de l'Estrie au Québec. Ces discours peuvent être obtenus soit de notre site Web, soit de nos locaux.

Comité sénatorial plénier : L'invitation la plus remarquable qu'ait reçu cette année (ou de tout temps) le Commissaire à la protection de la vie privée a été celle de comparaître devant le Comité sénatorial plénier, l'équivalent de son conseil d'administration. Le Commissaire à la protection de la vie privée fait en effet partie d'un petit groupe d'officiers nommés par le Parlement pour défendre l'équité, le sens moral et l'honnêteté dans l'administration publique, et qui doivent lui rendre des comptes.

Selon le Commissaire, la convocation de témoins devant des comités pléniers, autrefois pratique courante, semble s'être démodée. Il admet que ce pourrait bien être par souci d'efficience mais, à son avis, cela a eu le funeste effet de rendre moins visibles au public le processus législatif et les rouages du gouvernement.

Le Commissaire a brossé un bref portrait de la protection de la vie privée au pays, puis a affronté les questions et commentaires des sénateurs sur toute une foule de sujets, de sa défense du caractère confidentiel des questionnaires de recensement aux propositions de pré-contrôle par les douaniers américains dans les aéroports canadiens.

Nouvelle Constitution en Thaï lande : L'adoption par la Thaïlande d'une nouvelle Constitution a fourni au Commissariat une occasion unique de communiquer ce qu'il a appris (et ce qu'il continue d'apprendre) à un pays qui

s'initie au droit de l'information. La Constitution thaïlandaise prévoit plusieurs mécanismes visant à rendre l'appareil gouvernemental plus transparent et plus responsable, y compris une commission des droits de la personne et des Ombudsmans. La Constitution prévoit également des tribunaux administratifs, dont l'un des plus vitaux est le "Bureau de l'information" (son nom officiel d'alors), qui aurait eu pour mission d'appliquer la loi nationale sur les documents officiels.

Dans le cadre du Programme de gestion publique de l'Agence canadienne de développement international, un haut fonctionnaire du Commissariat a été invité en Thaïlande pour décrire l'expérience canadienne en matière de droit de l'information. Après avoir pris la parole lors d'une conférence sur la nouvelle loi organisée par le Premier ministre et télédiffusée en mai 1998, il a pris part à plusieurs réunions visant à mettre sur pied le nouveau "Bureau de l'information". Après son retour, le gouvernement thaïlandais a décidé de renommer l'organisme et d'en faire le "Bureau de l'accès à l'information et de la Protection de la vie privée", et ce dernier aspect a pris une grande importance dans la prise de décisions des commissaires du Bureau.

Le directeur du Bureau et deux hauts fonctionnaires thaïlandais sont ensuite venus au Canada pour assister en direct à l'application de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*. Le haut fonctionnaire de notre Commissariat est retourné en Thaïlande plusieurs mois plus tard à l'occasion d'une conférence anniversaire pour y relater les leçons que le Canada a apprises et celles qu'il a ignorées. Par la suite, il a présenté un exposé à une université locale et a rencontré le personnel du Bureau et de divers ministères, traitant surtout des exigences concrètes de l'implantation de la loi : le recensement des banques d'information, la préparation de guides administratifs, et la conception de cours de formation. L'expérience a confirmé au personnel du Commissariat à quel point les droits à l'information sont cruciaux pour une démocratie, et à quel point les Canadiens les tiennent pour acquis ou les ignorent carrément.

Fusion entre la vie privée, les politiques et les technologies de l'information : Au début de 1999, le Commissaire à la protection de la vie privée et de ses employés ont participé à une série de quatre tables rondes organisées par l'Institut d'administration publique du Canada (IAPC). Des députés, des hauts fonctionnaires, des journalistes et des universitaires y ont discuté des tensions entre une fonction publique privilégiant une information plus abondante et de meilleure qualité au service d'un meilleur gouvernement et des citoyens craignant que cela n'engendre une ingérence et un contrôle

accrus de l'État. Le débat n'est pas nouveau et, comme l'a signalé l'IAPC, le dialogue pourrait être utile.

La première table ronde a établi le contexte, la seconde a porté sur la protection de la vie privée et l'évolution du rôle de l'État, la troisième avait pour thème l'intégration de multiples sources de données, et la quatrième a traité du partage entre le gouvernement et le secteur privé.

Beaucoup de gens souhaitent un gouvernement "efficient", tellement, en fait, qu'on se demande comment le gouvernement est devenu si inefficace. Les tables rondes tenaient pour acquis que l'intégration des systèmes informatiques et des bases de données permet un fonctionnement plus efficace et plus efficient; or ce point de vue lui-même est peut-être erroné. Plus d'information ne signifie pas nécessairement plus de sagesse. Ils étaient beaucoup moins nombreux à faire écho aux propos que la Cour suprême américaine a tenus concernant le rôle de la *Bill of Rights* de son pays. La Cour a estimé que ce rôle était de protéger les valeurs fragiles de citoyens vulnérables contre l'impérieux souci d'efficacité qui peut caractériser des fonctionnaires dignes d'éloge tout autant, sinon davantage, que des fonctionnaires médiocres.

Dans son allocution de présentation de la deuxième table ronde, le Commissaire a souligné le rôle que l'efficience devrait jouer dans le gouvernement, et le rôle des lois dans la protection des citoyens contre la poursuite trop enthousiaste d'une telle efficience. L'IAPC prévoit publier un compte-rendu détaillé des tables rondes dans les mois à venir.

Direction des Enquêtes et renseignements

Le Commissariat a reçu 3 105 plaintes pendant l'exercice 1998-1999. C'est la première fois que le nombre de plaintes dépasse la barre des 3 000, ce qu'expliquent deux facteurs. Le premier est la décision du gouvernement de confronter les déclarations de douane des voyageurs de retour au Canada avec les fiches de demande d'assurance emploi (voir en page 92).

En second lieu, plus de 225 plaintes de retard ont été déposées par des employés de Services correctionnels Canada (SCC) travaillant au pénitencier québécois de Cowansville. Ils avaient présenté plus de 900 demandes de consultation de leur dossier personnel au cours de négociations contractuelles. Afin de réduire les formalités administratives, SCC avait établi des rendez-vous de consultation avec les employés au lieu de leur remettre des photocopies de leurs documents. La *Loi sur la protection des renseignements personnels* permet la consultation des originaux et, dans les circonstances, cette mesure était raisonnable considérant que les employés se servaient de cette loi comme d'un moyen de pression.

Deux autres ministères qui, par le passé, avaient éprouvé des difficultés à se conformer aux délais prescrits semblent maintenant réaliser d'appréciables progrès. Le ministère de la Défense nationale et le ministère du Revenu ont créé des équipes de travail dans leur section d'Accès à l'information et Protection des renseignements personnels (AIPRP) au début de l'exercice, et leur initiative semble porter fruit. À la fin de l'exercice, le nombre des plaintes pour retard avait considérablement baissé. D'autres ministères devraient s'en inspirer.

Quelques cas

Les cas suivants illustrent le genre de plaintes que reçoit le Commissaire à la protection de la vie privée

Registre des divorces
Par suite de la plainte déposée par un avocat du Manitoba au sujet de la communication, par le ministère de la Justice, de son nom et de son adresse à Développement des ressources humaines Canada (DRHC), la méthode de notification des parties à un divorce du partage des crédits du Régime de pensions du Canada (RPC) a changé.

L'avocat s'est plaint de ce que le ministère de la Justice avait divulgué à tort son nom et son adresse à la Direction générale des programmes de la sécurité du revenu de DRHC. (Il s'est également plaint de ce que DRHC a recueilli incorrectement les renseignements de Justice Canada.) La divulgation s'est faite lors d'un transfert mensuel régulier de bandes informatiques du Bureau d'enregistrement des actions en divorce du ministère de la Justice à DRHC. Les bandes contenaient les noms et adresses des personnes demandant un divorce (ou ceux de leurs avocats), données fournies par les tribunaux provinciaux aux fins du Registre des divorces. Le ministère de la Justice tient à jour le Registre afin de repérer les demandes de divorce en double.

Notre enquête a révélé que le ministère de la Justice a, en janvier 1993, modifié son formulaire d'enregistrement des actions en divorce, afin d'obtenir l'adresse postale des demandeurs de divorce ou de leurs représentants juridiques. Ce ministère n'avait pas besoin des adresses pour tenir son Registre; il les recueillait uniquement pour aider DRHC à envoyer aux demandeurs des trousses de renseignements sur le partage des crédits du RPC. (Les couples qui ont divorcé après 1987 sont légalement tenus de partager équitablement tout crédit du RPC accumulé par les deux conjoints au cours de leur mariage.)

Le greffier du tribunal remplit les formulaires et, lorsque la demande est présentée, il envoie la partie 1 au ministère de la Justice afin d'émettre le certificat de mise à jour. Une fois le dossier clos au tribunal, le greffier remplit la partie 2 et l'envoie au Registre (des renseignements de nature non personnelle sont également envoyés à Statistique Canada). Le tribunal conserve la partie 3.

Le registre est considéré comme du domaine public. Lorsque seul le nom des avocats y était indiqué (par exemple, pour protéger les personnes qui fuyaient une relation violente), ces derniers devenaient des intermédiaires auxquels on envoyait de multiples exemplaires de trousses de renseignements à l'intention de leurs clients, répétant essentiellement ce que les avocats avaient déjà fait. Le plaignant reconnaît être tenu d'informer ses clients de leurs droits de présenter une demande de partage des crédits du RPC, mais croit que la façon dont il s'acquitte de ses responsabilités professionnelles ne concerne nullement Santé et Bien-être social Canada (le ministère anciennement responsable du RPC).

Ces dispositions ne répondent pas à plusieurs critères de protection des renseignements personnels. Il était évident que le ministère de la Justice ne recueillait pas les renseignements aux fins de son propre programme prévu

par la loi, mais au contraire qu'il agissait comme agent d'une tierce partie, à savoir DRHC (devenu légalement responsable du RPC). En outre, le ministère de la Justice ne recueillait pas les renseignements directement auprès des personnes concernées, mais auprès des tribunaux provinciaux. En général, la collecte directe assure plus d'exactitude et donne aux particuliers la possibilité de donner leur consentement ou de refuser de le faire. Enfin, le ministère de la Justice divulguait à DRHC, qui les recueillait, des renseignements inutiles sur les représentants juridiques des parties à un divorce.

En outre, la procédure ne protégeait pas nécessairement quelqu'un d'un conjoint violent. Au cours de notre enquête, une femme a présenté une demande de divorce et a demandé au tribunal de n'en informer son mari qu'après qu'elle ait quitté le pays. Le tribunal a acquiescé à cette demande, mais les renseignements ont été envoyés comme d'habitude au ministère de la Justice puis communiqués à DRHC. Le mari a alors reçu la trousse de renseignements avant que sa femme n'ait eu le temps de quitter le pays. Il semble qu'elle n'ait pas subi de conséquences graves, mais l'incident a incité les ministères à retarder de deux mois ou plus la divulgation des renseignements dans un premier temps, avant de se pencher sur une nouvelle procédure.

Les plaintes ont également soulevé la question de l'utilité d'une communication personnelle; des renseignements génériques sur le partage des crédits devraient suffire et être bien plus rentables; DRHC envoyait par la poste environ 100 000 trousses par an, à un coût approximatif de 500 000 $.

Les deux ministères ont reconnu qu'il y avait des problèmes de protection de la vie privée et ont entrepris de remédier à la situation. Toutefois, comme il demeure important de s'assurer que les parties à un divorce comprennent leurs droits et leurs responsabilités en matière de partage des crédits de pension, ils avaient l'intention de maintenir la procédure actuelle jusqu'à ce qu'ils trouvent une solution satisfaisante. Le Commissaire à la protection de la vie privée a jugé que les plaintes étaient fondées, mais a décidé de ne clore les dossiers qu'une fois cette solution trouvée.

En janvier 1999, le ministère de la Justice a demandé aux tribunaux de ne plus inscrire l'adresse des parties à un divorce sur les formulaires d'enregistrement des divorces, et ce, à compter du 1er février. Après avoir épuisé le stock d'anciens formulaires, les nouveaux imprimés ne contiendront pas de champ d'adresse. Même si le Registre continue d'afficher un champ

d'adresse (qu'il serait onéreux d'éliminer à ce stade), il n'y aura aucun renseignement à y saisir. Le champ sera éliminé dans le cadre d'un projet de refonte du système.

DRHC a souscrit à notre argument selon lequel les renseignements sur le partage des crédits ne doivent pas être envoyés à une adresse personnelle. Il a produit un feuillet de renseignements expliquant les droits en matière de partage des crédits du RPC qu'il fournit à Justice Canada aux fins de diffusion dans les tribunaux provinciaux. Ces derniers insèrent simplement le feuillet de renseignements dans l'enveloppe contenant le jugement de divorce. Cette procédure a un autre avantage en ce que DRHC prévoit ainsi faire des économies importantes.

Destruction d'échantillons d'ADN et de leur analyse

Une plainte qui semblait être d'un genre courant a soulevé une question à laquelle le Commissariat s'intéresse depuis 1996, soit la destruction des échantillons d'ADN fournis volontairement au cours d'enquêtes policières. Même si la plainte en soi n'était pas fondée, elle a poussé le Commissaire à faire pression sur la Gendarmerie royale du Canada afin que cette dernière établisse une politique nationale stipulant que les échantillons d'ADN fournis volontairement, ainsi que les résultats d'analyse qui s'y rapportent, doivent être détruits dès que la personne concernée n'est plus soupçonnée.

Depuis toujours, le Commissaire encourage la police à détruire les échantillons d'ADN fournis volontairement. De fait, il n'apprécie pas du tout cette notion de demander aux gens de "prouver leur innocence", procédé qui va à l'encontre de notre système juridique. Cependant, ceux qui se portent volontaires afin d'aider la police dans ses enquêtes méritent une protection rigoureuse.

La plainte est issue d'une enquête de la GRC sur plusieurs agressions sexuelles qui ont eu lieu à Vermilion (Alberta) en 1996. Dans le cadre de cette enquête, le détachement local de la GRC a demandé à environ 400 hommes de la collectivité de fournir volontairement des échantillons d'ADN à des fins d'analyse génétique préalables à une comparaison avec les échantillons recueillis sur les lieux des crimes. La communauté a même fortement poussé ses hommes à répondre à l'appel.

Le plaignant, un résidant de Vermilion qui avait d'abord refusé de fournir un échantillon de son sang avant d'accepter à contrecœur, avait ensuite demandé qu'on lui communique les renseignements concernant son échantillon et contenus dans les dossiers de la GRC. Il voulait également savoir si ces

renseignements avaient été versés dans d'autres banques de données d'ADN sous tutelle provinciale ou fédérale.

La GRC lui a alors refusé l'accès aux renseignements parce qu'elle les avait obtenus pendant qu'elle exerçait des fonctions de police municipale à Vermilion. Le paragraphe 22(2) de la *Loi sur la protection des renseignements personnels* empêche la GRC de divulguer tout renseignement obtenu dans l'exercice de fonctions de police provinciale ou municipale si la province ou la municipalité demande la confidentialité. Quatre provinces, la Colombie-Britannique, la Saskatchewan, le Manitoba et la Nouvelle-Écosse, ont renoncé à la confidentialité dans de tels cas, permettant ainsi aux personnes d'avoir accès aux renseignements qui les concernent en vertu de la loi fédérale.

En raison de cette situation, les plaignants sont dans une impasse : bien que la loi albertaine sur la protection des renseignements personnels soit généralement comparable à la loi fédérale, la province prétend que son application aux activités provinciales ne couvre pas la GRC en sa qualité de force policière provinciale ou municipale. En conséquence, aucun demandeur ne peut avoir accès à ses renseignements personnels sans que les autorités provinciales n'en donnent la permission à la GRC.

En l'espèce, une fois la demande du plaignant parvenue au siège national de la GRC à Ottawa, le personnel de l'AIPRP a demandé l'information visée au détachement de Vermilion. Ce dernier a répondu que l'échantillon avait été détruit, ce qu'Ottawa a alors choisi de ne pas indiquer au plaignant, préférant refuser de lui communiquer l'information en vertu du paragraphe précité. L'homme s'est alors plaint auprès du Commissaire à la protection de la vie privée. Cette plainte allait toutefois bien au-delà du refus de donner accès à l'information et remettait plutôt en question le droit de la GRC de conserver les renseignements en question.

Notre enquêteur a alors appris du policier que ce dernier ne s'opposait pas à ce que l'homme apprenne que son échantillon avait été détruit et qu'il n'était pas suspect. L'affaire aurait dû être réglée : l'homme obtiendrait les renseignements qu'il demandait, le commissaire saurait que l'échantillon avait été détruit et la GRC conserverait la dérogation qui la concerne. Mais la GRC a décidé de maintenir la dérogation invoquée, et la direction du Commissariat est alors intervenue et a obtenue que l'enquêteur de la GRC dise à l'homme ce qu'il était advenu de son échantillon.

Fait plus important cependant, le policier nous a confirmé que, même si l'échantillon avait été détruit, les imprimés des autoradiogrammes (représentation visuelle de l'échantillon), les notes de travail et les rapports de laboratoire demeureraient au dossier jusqu'à ce qu'un suspect soit jugé et reconnu coupable. Le Commissaire de la GRC nous a ensuite envoyé une confirmation écrite du fait que ces renseignements ne sont versés dans aucune banque de données électronique, mais qu'ils font partie du dossier de l'enquête utilisé, si nécessaire, pour la communication, les tribunaux et les appels.

De toute évidence, un volontaire semblait avoir moins de droits qu'une personne obligée par mandat (et donc soupçonnée du crime) de fournir un échantillon d'ADN : en effet, la GRC a l'habitude de détruire un échantillon obtenu en exécution d'un mandat, ainsi que les résultats de l'analyse de cet échantillon, dès que la personne n'est plus soupçonnée.

Ni le plaignant ni le Commissaire à la protection de la vie privée n'étaient satisfaits.

Notre Commissaire a de nouveau écrit à celui de la GRC afin de réaffirmer sa volonté de voir créée une politique nationale cohérente sur la destruction des échantillons fournis volontairement. La plainte est restée en suspens. Après plusieurs réunions, appels téléphoniques, messages électroniques et avis contradictoires de destruction de l'échantillon, la GRC a enfin confirmé que tous les renseignements relatifs au plaignant avaient été détruits. Toutefois, la GRC refusait toujours de l'en aviser.

Frustrée, la direction du Commissariat a demandé au ministère de la Justice de l'Alberta de renoncer, dans cette affaire, à sa convention de confidentialité avec la GRC, permettant ainsi à cette dernière de confirmer au plaignant que tous les renseignements avaient été détruits. La province a accepté.

Enfin, en août 1997, la GRC a modifié sa politique interne afin d'exiger que les échantillons d'ADN fournis volontairement et les résultats de leur analyse génétique soient détruits dès qu'une personne est innocentée.

Cette plainte a eu d'importantes retombées, bien que le commissaire l'ait considérée comme non fondée (puisque la *Loi sur la protection des renseignements personnels* interdit à la GRC de divulguer des renseignements obtenus dans l'exercice de fonctions de police provinciale ou municipale). En effet, tant la GRC que tous les futurs volontaires peuvent désormais être certains que

leurs échantillons d'ADN et les résultats d'analyse les innocentant ne se retrouveront pas dans un dossier policier.

Les cas d'agressions sexuelles n'ont toujours pas été résolus.

L'AE examine des passeports périmés, et bien plus

Une plainte déposée par un Québécois à l'effet qu'une enquêteuse de l'assurance emploi (l'AE) avait obtenu son passeport périmé du ministère des Affaires étrangères pour vérifier ses déplacements hors du Canada est un autre accroc dans la saga permanente du couplage des données entre le service des Douanes de Revenu Canada et l'AE. (voir en page 92).

Mais ce n'était que la pointe de l'iceberg. Lorsque l'enquêteuse de l'AE a découvert un déplacement du plaignant remontant au mois de février 1995, elle a demandé un rapport de solvabilité à Equifax qui lui a permis de découvrir que l'homme en question détenait les cartes de crédit de trois banques. Elle a envoyé par télécopieur une demande de renseignements aux banques, qui lui ont renvoyé des listes détaillées d'achats effectués à crédit à l'extérieur du Canada.

Ayant découvert un autre voyage effectué entre décembre 1994 et janvier 1995, elle a demandé à deux agences de voyage des renseignements sur tout voyage qu'elles auraient organisé pour le plaignant. Elle a également envoyé par télécopieur un message au ministère des Affaires étrangères lui demandant le passeport périmé du plaignant. Le Bureau des passeports lui a envoyé le document en lui demandant de le remettre à son ancien titulaire dès qu'elle n'en aurait plus besoin.

La question qui vient immédiatement à l'esprit est celle voulant savoir pourquoi le ministère des Affaires étrangères détenait un passeport périmé; normalement, les passeports périmés sont annulés et renvoyés à leurs titulaires. D'après la section de la Sécurité des passeports, le ministère conserve les passeports lorsqu'ils sont saisis à l'étranger, lorsqu'ils ne sont pas réclamés une fois émis, lorsqu'ils servent à aider illégalement des étrangers dans d'autres pays, ou encore lorsqu'un nouveau passeport est émis pendant que l'ancien est encore valide. (Il semble que certains pays exigent des voyageurs qui se présentent à leurs frontières qu'ils aient un passeport en vigueur depuis trois à six mois au moins.) La durée pendant laquelle le ministère des Affaires étrangères conserve un passeport dépend des circonstances qui s'appliquent.

Le partage de renseignements, c'est simple : vous me dites tout sur vous, et je vous dis quand arrêter.

Le fichier informatique du plaignant ne contenait rien d'anormal susceptible de justifier la conservation de son passeport. Il indiquait qu'un nouveau passeport avait été émis et que l'ancien avait été annulé.

Le personnel du ministère des Affaires étrangères n'a pas pu expliquer pourquoi il a demandé à DRHC de remettre le passeport au plaignant une fois l'enquête de l'AE terminée. De toute évidence, il n'avait pas suivi sa politique consistant à transmettre toutes les demandes d'enquête de ce genre à son unité d'AIPRP. Cette dernière a profité de l'incident pour rappeler au employés des Passeports de suivre la procédure. Une question plus importante à élucider est celle de savoir s'il était inapproprié de transmettre le passeport à DRHC. Le Commissaire a conclu que le ministère des Affaires étrangères était en présence d'une demande invoquant des pouvoirs

d'enquête élargis prévus dans une autre loi du Parlement, et que le ministère ne pouvait donc pas être blâmé pour avoir transmis le document.

La Cour fédérale doit maintenant décider si DRHC aurait dû effectuer le couplage de sa base de données de l'AE avec les déclarations faites au service des Douanes par les voyageurs qui reviennent au Canada, processus qui l'a amené à recueillir tous ces renseignements.

Ce à quoi peut mener la perte d'un certificat de naissance

Un avocat de Montréal s'est plaint au Commissaire de ce que la Commission de l'immigration et du statut de réfugié (la CISR) avait non seulement refusé que sa cliente consulte les renseignements personnels la concernant, mais ne lui avait pas non plus renvoyé son certificat de naissance. L'enquête a mis en lumière plusieurs problèmes relatifs à la demande ayant donné lieu à la plainte, ainsi qu'à la façon dont la CISR gère ses dossiers.

L'avocat avait demandé au préposé à la demande de statut de réfugié copie de toute lettre ou toute note relative à l'authentification du certificat de naissance de sa cliente. L'intéressée avait demandé le statut de réfugié, et la CISR avait amorcé une audience informelle (traitement accéléré). Lorsque la CISR a décidé de faire authentifier le certificat de naissance de l'intéressée par Citoyenneté et Immigration Canada (CIC), elle a fait savoir à celle-ci que cela signifiait qu'elle devrait suivre la procédure normale d'audience.

Après plusieurs mois, l'avocat a demandé où en était le traitement de la demande. Le préposé de la CISR a confirmé qu'il avait envoyé le certificat de naissance pour authentification. L'avocat a alors déposé une demande formelle d'accès aux renseignements personnels de sa cliente avant d'obtenir de la CISR les 26 pages que contenait le dossier de demande du statut de réfugié. Le dossier ne faisant aucune mention du certificat de naissance original, et l'avocat ne pouvant pas croire ses yeux, il a alors porté plainte auprès de notre Commissariat.

Notre enquêteur a eu de nombreuses discussions avec des employés de la CISR et de CIC, qui ont tous maintenu que la vérification se poursuivait. La CISR a réitéré que le certificat de naissance ne lui avait pas été renvoyé mais, peu après, le certificat de naissance a refait surface pendant l'audience, qui venait d'être retrouvé dans un de ses dossiers. Très sceptique, notre enquêteur a alors demandé de consulter tous les dossiers originaux afin de retracer le cheminement du certificat de naissance. La CISR a produit deux dossiers : un principal destiné au membre présidant l'audience, et un double.

Les dossiers ne renfermaient aucune note, information administrative ni trace de suivi. Ils contenaient toutefois une note de service de CIC, datant de près d'un an, indiquant que le certificat de naissance était un faux, mais sans rapport d'authentification ni aucune mention de l'endroit où l'original avait été envoyé.

D'autres problèmes ont fait surface pendant l'examen de notre enquêteur. Il semble que le dossier avait été confié à un autre préposé aux demandes de statut de réfugié plus d'un an auparavant, mais personne n'avait signalé ce fait à l'enquêteur. Avant le transfert, le premier préposé avait retiré du dossier toute note ou observation susceptible d'influencer le nouveau préposé, mettant ainsi notre enquêteur dans l'impossibilité de confirmer si de l'information relative à la demande originale avait figuré au dossier.

Le premier préposé a nié savoir que le certificat de naissance avait été retrouvé et renvoyé à sa propriétaire, et ne pouvait pas non plus expliquer comment pareille chose avait pu se produire. Certains des problèmes relevés semblent avoir découlé du fait qu'il avait établi son propre processus officieux d'authentification des documents par CIC. Comme ce préposé n'avait pas instauré de système de suivi, il avait accumulé plusieurs pièces d'identité originales qu'il ne pouvait pas rattacher à leur propriétaire légitime parce qu'il n'en comprenait pas la langue.

Le Commissaire a convenu que la plainte relative au refus d'accès au dossier était fondée. Il s'est particulièrement inquiété de la pratique de la CISR consistant à détruire systématiquement les notes et les observations manuscrites de ses employés. La décision de conserver ou non des notes peut être prise en fonction de l'objet de celles-ci. Si les notes sont utilisées à des fins administratives (soit ici afin de décider d'une demande de statut de réfugié), elles devraient être conservées. Les supprimer équivaut à retirer à quelqu'un de l'information d'une importance critique, et contrevient aux droits à la vie privée de cette personne.

Le Commissariat poursuit ses démarches auprès de la CISR afin de corriger cette situation.

Le MDN invoque trop le secret professionnel

Un des dossiers de cette année montre bien le problème auquel est confronté le Commissariat lorsque des organismes élargissent indûment la portée d'exceptions légitimes. En l'espèce, le ministère de la Défense nationale (le MDN) a invoqué le secret professionnel (article 27 de la *Loi sur la protection des*

renseignements personnels) pour refuser à un membre des Forces armées l'accès aux procédures d'une Commission enquêtant sur ses plaintes.

Le MDN aurait mal géré les plaintes de harcèlement et de négligence médicale portées par le membre, ce qui a engendré un long conflit entre le MDN et le plaignant. Ce dernier a demandé nombre de fois à avoir accès à des renseignements médicaux. On lui avait déjà fourni beaucoup de documents et même, à un certain moment, la possibilité d'examiner tout le dossier. Toutefois, le conflit s'est intensifié et le membre a déposé un grief comportant une importante demande d'indemnisation financière par le MDN.

Comme il s'agissait d'une somme considérable, le MDN a traité le grief comme une demande contre la Couronne. Le MDN a établi une Commission d'enquête afin qu'elle recueille la preuve. Parallèlement, la procédure de grief a suivi son cours. Après sa comparution, le membre a demandé à avoir accès aux quelque 2 300 pages du dossier de la Commission. Le MDN a cependant refusé tout accès aux documents sous prétexte que l'ensemble de la procédure de la Commission, sauf ses conclusions et ses recommandations, était protégé par le secret professionnel.

Notre Commissaire n'a pas accepté une application aussi large de l'exception prévue à l'article 27 de la loi. La procédure consistait à recueillir des faits et était donc semblable à une enquête administrative. La divulgation des documents ne révélerait aucune des stratégies ni des analyses du MDN, ni aucun renseignement protégé par le secret professionnel. Il semblait y avoir une contradiction flagrante dans le fait d'appeler le membre à témoigner dans une procédure pour laquelle l'autre partie invoque ensuite le secret professionnel. Cette contradiction paraissait d'autant plus grande par ailleurs si le membre décidait d'intenter une action au civil, la plupart des documents devant alors lui être communiqués.

De longues négociations ont alors commencé. Notre Commissariat a demandé au MDN de communiquer tous les éléments de preuve purement factuels et de ne refuser l'accès qu'à ceux qui comportaient des avis juridiques. Le MDN a répliqué qu'il existait un précédent juridique selon lequel renoncer au secret professionnel pour un document signifiait y renoncer pour tous les documents du dossier. Apparemment dans une impasse, notre Commissaire a écrit au sous-ministre.

Le MDN n'était pas d'accord avec notre perception des travaux de sa Commission comme étant de nature administrative et visant à assurer un milieu de travail sain et libre de tout harcèlement. Le membre avait été relevé de ses fonctions militaires quelques années auparavant et était maintenant rendu à la vie civile pour des raisons médicales. Selon le MDN, le recours du membre ne visait nullement à améliorer le milieu de travail, mais bien à obtenir la plus grosse indemnisation possible pour les mauvais traitements qu'il aurait soi-disant subis. Le sous-ministre a écrit que la Commission avait été constituée pour réunir la preuve qui aiderait les avocats et les conseillers de la Couronne à déterminer la validité de la demande du membre; les renseignements étaient nécessaires pour fournir un avis juridique quant à la responsabilité de la Couronne et faisaient donc partie intégrante du dossier.

Malgré la différence de points de vue, le MDN a accepté de fournir au membre des copies de son propre témoignage, tous les documents traitant du harcèlement, son dossier médical ainsi que d'autres documents déjà reçus. Afin de clore le dossier, le MDN a décidé de cesser de recourir au secret professionnel et de divulguer la plupart des documents relatifs aux travaux de sa Commission.

Qui leur a donné mon nom ? Pas la Société canadienne des postes !
Dans ce cas précis, cette perpétuelle question que nous posons à notre boîte aux lettres n'a pas trouvé de réponse satisfaisante, et ce, malgré la bonne volonté manifestée par tous les intervenants à la Société canadienne des postes (SCP) et l'Association canadienne du marketing direct (ACMD) ainsi que par des courtiers en listes et une entreprise de marketing direct.

Un étudiant d'université de l'Alberta, qui avait vu le Commissaire à la protection de la vie privée à l'émission de télévision *Coast to Coast* (diffusée au réseau anglais de Radio-Canada), lui a écrit pour lui faire part d'envois bizarres que sa grand-mère avait reçus de la Californie. Pendant ses études de droit à Edmonton, il avait écrit certaines lettres à sa grand-mère vivant à Calgary en écrivant sur l'enveloppe un surnom affectueux en ukrainien au lieu de son prénom et de son nom de famille. Environ deux ans plus tard, celle-ci commençait à recevoir une foule d'envois non sollicités de la Californie adressés à son prénom assorti du surnom affectueux en ukrainien au lieu de son nom de famille : une combinaison donnant à peu près "Carole Mamie"!

Comme lui seul et des proches parents utilisent cette expression, et que sa grand-mère n'avait certainement jamais utilisé ce nom de façon officielle, l'étudiant a conclu que seule la SCP pouvait être la source de l'adresse. Notre enquêteur a donc entrepris de retracer l'origine du courrier.

La SCP s'est bien défendue de numériser les noms et les adresses figurant sur le courrier. D'abord, elle n'a pas le matériel voulu pour consigner les coordonnées de toute personne recevant du courrier. Ensuite, l'information réunie ne serait d'aucune utilité pour la SCP ni pour les entreprises de marketing direct, les particuliers constituant un groupe tellement nombreux et hétéroclite qu'il ne serait guère efficace de les cibler pour offrir des produits et des services.

Dans l'intervalle, la grand-mère a reçu un autre envoi portant ce drôle de nom, cette fois de l'organisme Rehandart Canada Ltd., représentant les personnes qui peignent avec leur bouche et leurs pieds. L'enquêteur a demandé à l'ACMD si elle avait une explication. L'ACMD s'est dite intriguée par le couplage du prénom et du surnom affectueux et a offert de soulever la question auprès de son pendant américain. L'enquêteur a écrit à Rehandart qui, tout en n'étant pas membre de l'ACMD, s'est empressé de fournir le nom du courtier en listes duquel l'organisme avait acheté ses adresses. Ce courtier a révélé l'identité du gérant de la liste, qui a pour sa part indiqué la source des renseignements : une entreprise vendant des bas culottes et des sous-vêtements par correspondance.

Le gérant de la liste a proposé de rayer le nom de la grand-mère et de déterminer à quel moment l'achat avait été effectué et quel était le nom inscrit sur la liste. Il a confirmé qu'une paire de bas culottes gratuite avait été commandée pour le nom en question, commande qui avait été suivie d'une autre, impayée, de plusieurs autres paires. La grand-mère a confirmé avoir fait une commande au moyen de son vrai nom (et dont le chèque avait été encaissé), mais qu'elle avait retourné la documentation relative à la commande plus volumineuse faite au nom incorrect. La base de données de l'entreprise contenait la bonne date de naissance, le bon numéro de téléphone et la bonne taille, mais pas le bon nom.

Le courtier en listes de Rehandart a ensuite trouvé le nom exact de l'intéressée sur la liste "Lifestyle Selector", constituée à partir de bons de garantie. La piste a finalement disparue aux États-Unis, où le *Cash Disbursement Centre* (une entreprise de tirages au sort) de Laguna Hills, en Californie, n'a pas donné suite aux deux demandes faites par l'ACMD relativement à la provenance de sa liste.

Il est évident que l'information ne provenait pas de la SCP, ce que rien ne pouvait prouver et ce que corroborait l'opinion unanime des courtiers en listes, des gérants des listes et de l'ACMD. Le Commissaire sait gré à ces

entreprises privées des efforts considérables qu'elles ont déployés dans ce dossier.

Mais alors, qui leur donne nos noms? Nous-mêmes, par le biais de presque toutes les revues auxquelles nous nous abonnons, tous nos achats faits par catalogue et tous les bons de garantie que nous remplissons. Tous ces renseignements se retrouvent sur une liste quelque part. Si vous ne voulez pas figurer sur les listes de marketing direct, faites-le clairement savoir au moment de l'achat. La plupart des entreprises de bonne renommée respecteront votre volonté. Pour faire rayer votre nom des listes des membres de l'ACMD, il suffit d'écrire à :

Association canadienne du marketing direct
1 Concorde Gate, Suite 607
Don Mills (ON) M3C 3N6

Disparition de notes d'enquête suite à une plainte de harcèlement
Il arrive parfois que l'animosité personnelle qui donne lieu à des accusations de harcèlement se répercute sur la façon dont un ministère traite les demandes de communication de renseignements qui en découlent inévitablement.

Dans un de ces cas, une employée a déposé plusieurs plaintes selon lesquelles Environnement Canada lui avait refusé accès à des documents concernant son rendement et ses compétences. Elle avait également demandé à voir tout document portant sur la façon dont le ministère avait traité une plainte de harcèlement qu'elle avait déposée ainsi que les documents relatifs à la décision de déclarer le poste qu'elle occupait «affecté» (c'est à dire excédentaire). Les accusations de harcèlement découlaient de la réponse fournie par la direction aux allégations d'irrégularités dans la classification de postes, accusations pour lesquelles le ministère a refusé de recourir à la médiation offerte par la Commission de la fonction publique.

Dans une plainte, l'intéressée déplorait la disparition de déclarations de témoins et de notes d'entrevues qu'avait réunies un entrepreneur indépendant ayant été recruté pour mener enquête au sujet de ses accusations de harcèlement. Des documents figurant dans les dossiers de l'un des deux gestionnaires nommés dans la demande de communication avaient également disparu.

L'enquêteur à la protection de la vie privée a confirmé que la plupart des déclarations manuscrites des témoins semblaient avoir disparu des dossiers

du ministère, où elles auraient dû être conservées. L'entrepreneur a insisté sur le fait qu'il les avait remis tous ces documents au ministère, et un témoin a confirmé les avoir vus. Mais on n'a pu trouver que les déclarations dactylographiées et non signées. La plaignante voulait voir les originaux signés au lieu des versions dactylographiées établies par la suite.

L'enquêteur a aussi remarqué que des pages semblent avoir été supprimées dans l'information reçue par la plaignante, et sans explication à ce sujet. Il semble que l'entrepreneur avait reçu l'information incomplète de l'un des gestionnaires. L'enquêteur a demandé à voir les documents manquants, demande qui a reçu un accueil glacial de la part du gestionnaire. Pendant la discussion enflammée qui a suivi, celui-ci a prétendu que l'information et le dossier d'accompagnement (qu'il a montré à l'enquêteur, mais qu'il ne lui a pas permis d'examiner) représentaient ses notes personnelles. Il a menacé de les détruire si la plaignante demandait à les consulter. Étant donné qu'il n'était qu'à quelques mois de la retraite, il a soutenu n'avoir rien à perdre et qu'il ne subsisterait aucune preuve de son geste.

L'enquêteur a prévenu le gestionnaire que, qu'elle soit de nature personnelle ou non, l'information constituait un document ministériel et était assujettie à la *Loi sur la protection des renseignements personnels*. Pour les fonctionnaires, cette affirmation représente souvent une révélation. L'information que les fonctionnaires réunissent pendant leur emploi à des fins liées au travail constitue un document gouvernemental, et non pas personnel. L'enquêteur a conseillé au gestionnaire de consulter un avocat avant de poser le geste risqué et illégal consistant à détruire les documents. Bien qu'un gestionnaire de plus haut niveau ait confirmé l'affirmation de l'enquêteur, et que le personnel ait entrepris de réunir l'information, le conseil semble être tombé dans l'oreille d'un sourd, l'enquêteur ayant en effet appris plus tard que le gestionnaire avait « égaré son dossier ».

Cette réponse a fait atterrir le problème sur le bureau du sous-ministre adjoint (SMA). L'ordinateur et le bureau du gestionnaire ont été fouillés, tout comme un étage entier au cas où des boîtes de dossiers du gestionnaire auraient été transportées dans le mauvais bureau pendant un récent déménagement. Bien qu'on ait trouvé des documents originaux et des notes manuscrites, l'enquêteur n'a pas pu confirmer qu'il s'agissait de la totalité des documents figurant dans le dossier du gestionnaire. Le SMA a ensuite rencontré le gestionnaire pour faire ressortir l'obligation juridique lui incombant de produire les documents.

Oups ! Il semblerait que votre dossier ait été détruit automatiquement...

Finalement, le gestionnaire a signé une déclaration assermentée énumérant les documents qu'il avait en sa possession au moment de sa rencontre avec l'enquêteur et à l'effet qu'il n'avait détruit aucun document relatif à l'affaire. Malheureusement, c'était trop peu, trop tard. Le ministère aurait dû examiner les documents et communiquer la plupart de ceux-ci bien avant sa réponse à la demande initiale de la plaignante.

L'enquêteur a ensuite suivi la piste des déclarations manuscrites et signées des témoins. L'entrepreneur a réitéré qu'il les avaient toutes remises au ministère. Comme plusieurs entrevues avec des employés n'avaient rien donné, la direction du Commissariat a demandé à rencontrer le sous-ministre. Cette demande a donné lieu à une autre fouille, qui a fait apparaître les vingt déclarations manuscrites ainsi que les notes qu'avait prises l'entrepreneur pendant son entrevue avec la plaignante. Le ministère a traité les documents et a envoyé ceux-ci à la plaignante presque quatre ans après sa première demande.

Le ministère avait manifestement tort quand il a maintenu qu'il avait remis à la plaignante tous les documents auxquels elle avait droit; il n'avait pas fait de

démarches auprès d'une source évidente que l'intéressée avait nommée dans sa demande. Et l'entrepreneur avait affirmé deux fois à l'enquêteur qu'il avait remis tous les documents. On n'a jamais pu établir où se cachaient les documents pendant la conduite de l'enquête. Vu la façon dont sa demande de communication a été traitée, la nécessité de faire intervenir le Commissariat à plusieurs reprises et le temps qu'il a fallu au ministère pour produire les documents, on peut comprendre le mécontentement de la plaignante à l'égard de tout le processus. On peut aussi comprendre qu'elle continue de croire qu'il reste d'autres renseignements pertinents.

Comme on pouvait s'y attendre, la plainte était fondée.

Il faut d'abord expliquer, puis obtenir le consentement

Deux plaintes illustrent l'importance pour les ministères d'obtenir le consentement explicite d'une personne avant de recueillir des renseignements personnels d'autres organismes ou de leur en communiquer. Comme les conséquences peuvent souvent être graves pour les particuliers, ils doivent être parties prenantes au processus.

Compromettre une enquête et un futur emploi
Un camionneur a présenté une demande d'assurance emploi (AE) à Développement des ressources humaines Canada (DRHC). Sur la demande, il a indiqué qu'il avait démissionné de son emploi parce que son entreprise lui demandait de travailler un plus grand nombre d'heures que le maximum autorisé par la loi provinciale. Il avait également déposé une plainte détaillée auprès du ministère provincial des Transports, qui avait convenu de la traiter en toute confidentialité. Ce ministère avait indiqué qu'il effectuerait une vérification de l'entreprise incriminée.

Une agente de l'AE a téléphoné au demandeur lui demandant des preuves de ses allégations, ainsi que toute correspondance entre le ministère des Transports et lui. Elle lui a ensuite dit qu'elle communiquerait avec son ancien employeur.

Le demandeur a expliqué en long et en large à l'agente les problèmes que susciterait le fait d'entrer en communication avec son ancien employeur, la divulgation de renseignements pourrait compromettre la vérification du ministère des Transports, de même que son propre avenir dans l'industrie du camionnage. Il a donc refusé de donner plus de renseignements avant de

consulter son avocat et son député, ce à quoi l'agente lui a rétorqué que, sans les renseignements, elle refuserait sa demande de prestations.

Trois jours plus tard, l'agente de l'AE (qui avait 14 jours pour traiter la demande de prestations) a communiqué avec l'ancien employeur du camionneur. Le ministère lui a initialement refusé les prestations, car il avait quitté son emploi « sans motif valable ». L'homme en a appelé de la décision et un conseil arbitral a renversé cette dernière.

En vertu de la *Loi sur l'assurance emploi***,** DRHC est autorisé à recueillir des renseignements en vue d'établir que les demandeurs sont admissibles aux prestations. Par souci d'équité de la procédure, il doit également donner la possibilité aux employés et aux employeurs de donner leur version des faits. Au stade de la présentation de la demande, on demande aux employeurs leur version des faits et de corroborer ou de réfuter les déclarations des employés. Si des décisions font l'objet d'un appel, toutes les parties intéressées reçoivent tous les documents que le conseil arbitral étudiera.

Même si le camionneur n'a pas explicitement dit à l'agente de l'AE d'arrêter de traiter sa demande, le Commissaire à la protection de la vie privée a considéré qu'il lui avait expliqué avec suffisamment de clarté que les circonstances de son cas étaient tout à fait particulières. Elle aurait dû suspendre le processus en attendant de parler au ministère provincial des Transports de la vérification que celui-ci devait effectuer et de recevoir des instructions claires du camionneur qu'il était prêt à aller de l'avant avec sa demande, et à subir les conséquences éventuelles.

Le Commissaire a conclu que la plainte était fondée parce que le ministère avait omis d'adapter sa recherche de faits aux circonstances du cas (comme l'exige sa propre politique) et a divulgué des renseignements sans le consentement du demandeur à son ancien employeur. Il souhaitait également éviter qu'un tel incident se reproduise. Notre enquêteur cherche à faire apporter des changements aux procédures de DRHC, permettant aux demandeurs de prestations d'AE de retirer ou de suspendre leurs demandes. Notre enquêteur tente également de faire modifier le formulaire de demande de prestations pour qu'il indique clairement que la signature du demandeur équivaut à une autorisation à communiquer avec l'ancien employeur.

À court terme, DRHC doit diffuser un bulletin conseillant à son personnel de s'assurer que les clients savent que l'on communiquera avec leur ancien employeur. DRHC envisage également de réviser sa brochure et son

formulaire de demande d'AE pour éclaircir tout cela. Rien n'a encore été fait au moment où nous imprimons ces lignes.

La CISR a besoin d'un consentement explicite

Une demandeuse du statut de réfugié s'est retrouvée dans des circonstances un peu semblables après que Citoyenneté et Immigration Canada (CIC) eut transmis sa demande à la Commission de l'immigration et du statut de réfugié (CISR). Elle a rempli les formulaires nécessaires et, après une première attente, a retenu les services d'un avocat. Un préposé aux demandes de statut de réfugié a examiné sa demande et a recommandé une évaluation complète des risques au président du conseil d'examen. Une telle évaluation sert généralement à déterminer les dangers qu'encourrait le demandeur s'il était renvoyé dans son pays d'origine. Le président du conseil d'examen a rejeté cette recommandation parce que la femme faisait sa demande à partir des États-Unis : il aurait été inusité pour la CISR d'effectuer des évaluations des risques dans un pays ami. On a conclu qu'une vérification du casier judiciaire suffisait.

La CISR a informé l'avocat de la femme de son intention d'effectuer la vérification et lui a demandé s'il avait la moindre objection. Malheureusement, l'avocat a laissé tomber le cas une semaine après avoir reçu l'avis et n'a pas formulé d'objection. Ne recevant aucune nouvelle, la CISR a demandé à la Gendarmerie royale du Canada (GRC) d'effectuer la vérification du casier judiciaire. La femme n'a appris cette démarche que deux mois plus tard, alors qu'elle allait chercher les dossiers chez l'avocat. Très contrariée, elle s'est plaint de ce que, en demandant à la GRC d'effectuer la vérification, la CISR avait communiqué au *Federal Bureau of Investigations* (FBI) américain l'endroit où elle se trouvait, compromettant ainsi sa sécurité.

Notre enquêteur a déterminé que la GRC avait donné suite à la demande de la CISR en vérifiant ses propres dossiers et non la base de données du FBI. Les renseignements figuraient dans la base de données de la GRC parce que CIC avait demandé une vérification semblable avant de transmettre le cas à la CISR. À ce stade, la GRC avait demandé de l'aide au FBI. Notre Commissaire a conclu que la CISR avait le droit de demander des renseignements à la GRC et n'était pas la source de la divulgation. La plainte n'était donc pas fondée.

Toutefois, la décision d'effectuer la vérification sans que l'intéressée n'ait explicitement donné son consentement est troublante. Il serait très dangereux pour certains demandeurs du statut de réfugié de considérer que leur silence

équivaut à leur consentement à recueillir davantage de renseignements. La CISR doit changer ses lignes directrices afin d'obtenir le consentement explicite des demandeurs et leur donner le choix de retirer leur demande avant qu'elle ne cherche à obtenir des renseignements supplémentaires. Le Commissariat poussera la question auprès de la CISR.

Une divulgation inacceptable du rendement d'une tierce partie
Une employée d'un des Centres de formation de Services Correctionnels Canada (SCC) a démissionné, alléguant de conditions de travail intolérables. Dans sa demande de prestations d'assurance emploi (AE), elle a cité le nom d'un collègue qui serait en mesure de corroborer son évaluation du milieu de travail.

SCC en a appelé de la décision du conseil arbitral d'octroyer des prestations d'AE. De plus, le ministère a tenté de discréditer le collègue auprès des membres du conseil en remettant à Développement des ressources humaines Canada (DRHC) plusieurs documents détaillant les absences et le rendement du collègue, ainsi que la décision de ne pas renouveler son contrat.

Cependant, cet homme n'ayant jamais été appelé à témoigner, sa crédibilité n'était d'aucune importance. Si SCC avait tenté de prouver son parti pris, le ministère n'avait qu'à révéler le non-renouvellement de son contrat aux membres du conseil arbitral, au lieu d'y rajouter une quantité excessive de détails personnels ayant mené à une telle décision. En bout de ligne, SCC a peut-être même souffert de cette divulgation, laquelle ne faisait que confirmer les problèmes du milieu de travail. Le conseil arbitral a donc maintenu sa décision d'accorder des prestations à l'ancienne employée.

Le Commissaire trouve que la divulgation de SCC constitue un grave manquement à la loi. Les documents ayant été divulgués, cependant, le Commissaire a reconnu son impuissance à réparer les torts causés au collègue. SCC a présenté ses excuses à ce dernier et a convaincu DRHC de détruire tous les documents le concernant dans les dossiers d'appels en matière d'AE.

Le calendrier du mari pour vérifier la demande de sa femme
Un homme de Calgary s'est plaint de ce que la Société canadienne des postes SCP) avait communiqué son calendrier de vacances à la Commission des accidents du travail (CAT), laquelle menait enquête au sujet de la demande de prestations d'invalidité prolongée de son épouse.

L'épouse, qui est aussi à l'emploi de la SCP, était en période d'invalidité prolongée après d'avoir été victime d'un vol à main armée plusieurs années auparavant. Suite à l'incident, elle présentait plusieurs problèmes de santé, dont une angoisse prononcée, de l'agoraphobie et des crises de panique. Ces problèmes l'empêchaient de retourner au travail malgré les efforts considérables déployés par la SCP pour modifier son emploi. La femme soutenait qu'elle ne pouvait quitter son domicile que lorsqu'elle était accompagnée de parents ou d'amis.

L'invalidité prolongée, qui semblait aller en s'aggravant, et la demande de prestations illimitée ont incité la CAT à recourir aux services d'un détective privé pour surveiller l'intéressée (y compris en la filmant en train de vaquer à ses occupations). Dans le cadre de son enquête, la CAT a demandé à la SCP de lui fournir le calendrier de vacances du mari afin de pouvoir observer l'intéressée pendant les vacances familiales.

La SCP est dans l'obligation de coopérer avec les enquêtes des commissions provinciales des accidents du travail et de fournir à ces dernières les renseignements voulus pour le traitement des demandes de prestations. Cependant, la SCP doit également s'assurer que toute information qu'elle communique à la CAT, particulièrement au sujet de tiers, est pertinente à la demande. Bien que la CAT ait indiqué qu'elle seule peut juger de la « pertinence » d'un renseignement, la SCP doit aussi respecter la *Loi sur la protection des renseignements personnels*. La SCP ayant recueilli les renseignements pour l'administration des crédits de congé annuel et des horaires de travail de ses employés, leur divulgation à la CAT dans le cadre d'une enquête au sujet de la demande de prestations d'une tierce personne est une tout autre affaire. Le Commissaire n'a donc pas été convaincu de la « pertinence » des renseignements et a conclu que la plainte était fondée.

Demandes de renseignements

Les demandes de renseignements se sont pratiquement stabilisées à 10 313 l'année dernière. Toutefois, certains sujets ont suscité plus d'intérêt que d'autres, dont le numéro d'assurance sociale, l'accès aux données du recensement de 1911, le Bureau d'enregistrement des armes à feu, et le projet de loi C-54 relatif à la protection des données dans le secteur privé. Le jugement relié à la divulgation par Revenu Canada des déclarations de douane des voyageurs (voir en page 92) a donné lieu à de nombreux appels de gens voulant savoir les conséquences de la décision tant pour les individus ayant

déposé une plainte auprès de notre Commissariat que pour l'avenir du couplage de données. Le gouvernement a porté le jugement en appel.

Les demandes relatives au numéro d'assurance sociale ont presque doublé, peut-être en raison des critiques formulées par le Vérificateur général eu égard à son administration, et de ses commentaires quant aux conséquences de cette administration sur la vie privée (voir en page 19).

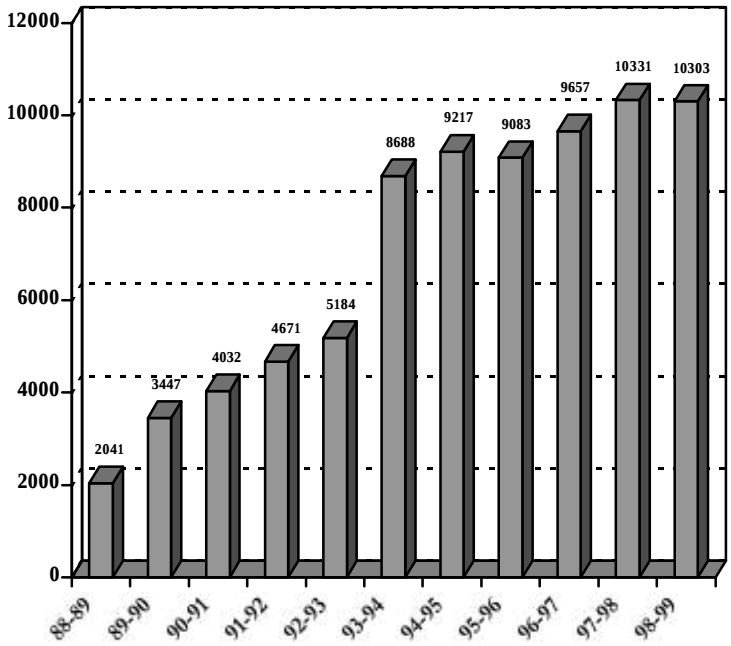
Depuis le mois de décembre 1998, les acheteurs d'armes à feu et de nombreux propriétaires actuels ont reçu des formulaires d'inscription du Bureau d'enregistrement des armes à feu. Beaucoup des personnes nous ayant téléphoné étaient préoccupées par le niveau de détail du formulaire, par l'utilisation qui serait faite des données et par la façon dont le Bureau protégerait les renseignements. Le Commissaire à la protection de la vie privée avait soulevé beaucoup de ces mêmes questions devant les comités du Sénat et de la Chambre des communes ayant révisé la loi constituant le Bureau. Ni cette loi ni ses règlements d'application subséquents ne fournissent de détails, laissant ainsi beaucoup de ces questions sans réponse et mécontentant par le fait même tant les propriétaires d'armes à feu que le Commissaire.

Le tableau à la page suivante donne un aperçu des diverses catégories de demandes de renseignements.

Demandes de renseignements par type

Loi, interprétation & application	4 399
Aucune compétence fédérale	275
Aucune compétence, secteur privé	503
Acheminées au commissaire provincial	885
Acheminées à un autre organisme fédéral	226
Acheminées ailleurs	97
Numéro d'assurance sociale	819
Institutions financières, assurance, crédit	383
Télécommunications	127
Marketing direct	80
Dossiers criminels, pardons, dérogations américaines	142
Médical	79
Adoption, généalogie, personnes portées disparues	108
Autres	405
Affaires publiques (médias, publications)	1 775
TOTAL	**10 303**

Demandes de renseignements 1988-1999



Les dix ministères les plus visés selon les plaintes reçues

		Motifs		
Ministère	**TOTAL**	**Accès**	**Délais**	**Vie privée**
Développement des ressources humaines Canada	1 028	50	65	913
Service correctionnel Canada	672	178	455	39
Revenu Canada	665	58	127	480
Défense nationale	180	50	108	22
Commission d'appel de l'immigration	121	23	74	24
Gendarmerie royale du Canada	103	73	12	18
Citoyenneté et immigration Canada	64	26	33	5
Service canadien du renseignement de sécurité	48	33	12	3
Société canadiennes des Postes	29	8	6	15
Justice, Ministère de la	28	10	7	11
AUTRE	167	80	44	43
TOTAL	**3 105**	**589**	**943**	**1 573**

Plaintes réglées par motifs, et résultats

	Résultats						
Motifs	**Fondée**	**Fondée; résolue**	**Non fondée**	**Aban-donnée**	**Résolue**	**Réglée**	**Total**
Accès	**10**	**86**	**303**	**47**	**30**	**218**	**694**
Accès	10	84	293	38	29	211	665
Correction/Annotation	0	2	10	9	0	5	26
Frais contre-indiqués	0	0	0	0	0	1	1
Répertoire	0	0	0	0	0	0	0
Langue	0	0	0	0	1	1	2
Atteinte à la vie privée	**43**	**6**	**60**	**27**	**13**	**67**	**216**
Collecte	15	0	15	6	4	20	60
Conservation/Retrait	1	0	5	1	0	6	13
Usage & Communication	27	6	40	20	9	41	143
Délais	**908**	**3**	**57**	**18**	**0**	**29**	**1 015**
Correction/Délais	25	0	0	0	0	18	43
Délais	873	3	45	17	0	11	949
Avis de prorogation	10	0	12	1	0	0	23
TOTAL	**961**	**95**	**420**	**92**	**43**	**314**	**1 925**

Plaintes réglées par institutions et résultats

Institution	Total	Fondée	Fondée; résolue	Non-fondée	Aban-donnée	Résolue	Réglée
Agriculture et Agro-alimentaire Canada	3	1	1	0	0	0	1
Affaires étrangères et Commerce international	11	1	1	5	0	0	4
Affaires indiennes et du Nord Canada	1	0	0	0	0	0	1
Anciens combattants Canada	11	0	0	4	3	0	4
Archives Nationales du Canada	9	1	0	1	1	0	6
Banque du Canada	1	0	0	0	0	0	1
Bureau du Conseil Privé	9	5	0	3	1	0	0
Bureau du directeur général des élections	1	0	0	1	0	0	0
Citoyenneté et immigration Canada	60	16	10	13	3	4	14
Commissariat aux langues officielles	1	1	0	0	0	0	0
Commission canadienne des droits de la personne	3	0	1	1	0	0	1
Commission de contrôle de l'énergie atomique	1	0	0	0	0	0	1
Commission de l'immigration et du statut du réfugié	123	86	5	9	0	0	23
Commission de la fonction publique	21	8	2	3	4	1	3
Commission des plaintes du public contre la GRC	6	0	0	4	0	1	1
Commission nationale des libérations conditionnelles	19	5	0	6	1	2	5
Conseil du trésor du Canada	2	1	0	1	0	0	0
Défense nationale	246	168	12	28	1	3	34
Développement des ressources humaines Canada	141	45	6	13	12	0	65
Environnement Canada	24	10	4	10	0	0	0

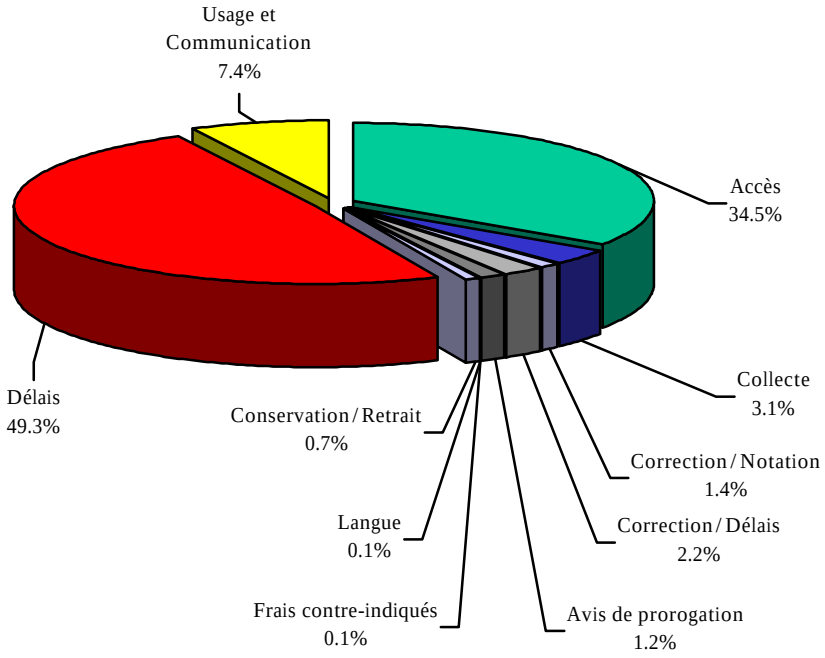
Plaintes réglées par institutions et résultats (suite)

Institution	Total	Fondée	Fondée; résolue	Non-fondée	Aban-donnée	Résolue	Réglée
Gendarmerie royale du Canada	98	5	5	43	10	1	34
Industrie Canada	6	0	1	2	2	1	0
Justice, Ministère de la	45	3	6	20	7	2	7
Office de commercialisation du poisson d'eau douce	1	0	0	1	0	0	0
Patrimoine Canada	2	0	0	0	0	0	2
Pêches et Océans	5	3	0	0	1	0	1
Ressources naturelles Canada	6	0	2	2	0	0	2
Revenu Canada	241	148	14	46	9	0	24
Santé Canada	10	4	1	3	1	0	1
Service canadien du renseignement de sécurité	48	8	4	19	0	0	17
Service correctionnel Canada	679	424	13	147	35	18	42
Société canadienne d'hypothèques et de logement	1	0	0	0	0	0	1
Société canadienne des Ports	1	0	0	0	0	0	1
Société canadienne des Postes	35	3	2	13	0	3	14
Société du crédit agricole Canada	4	1	1	1	1	0	0
Solliciteur général Canada	8	0	0	7	0	1	0
Statistiques Canada	20	4	1	8	0	6	1
Transports Canada	10	4	2	4	0	0	0
Travaux publics et Services gouvernementaux Canada	12	6	1	2	0	0	3
TOTAL	**1 928**	**961**	**95**	**420**	**92**	**43**	**314**

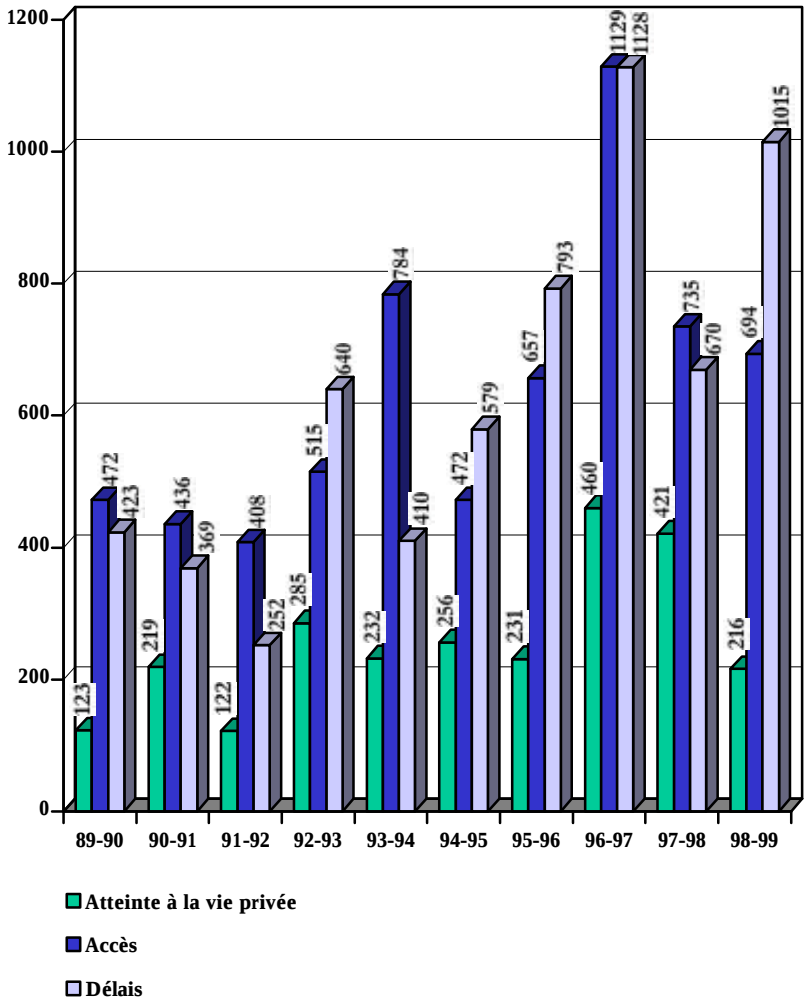
Origine des plaintes réglées

Terre-Neuve	12
Île-du-Prince-Édouard	3
Nouvelle-Écosse	77
Nouveau-Brunswick	23
Québec	631
Région de la capitale nationale – Québec	13
Région de la capitale nationale – Ontario	180
Ontario	442
Manitoba	54
Saskatchewan	101
Alberta	78
Colombie-Britannique	299
Territoires du Nord-Ouest	0
Yukon	0
Hors Canada	12
TOTAL	**1 925**

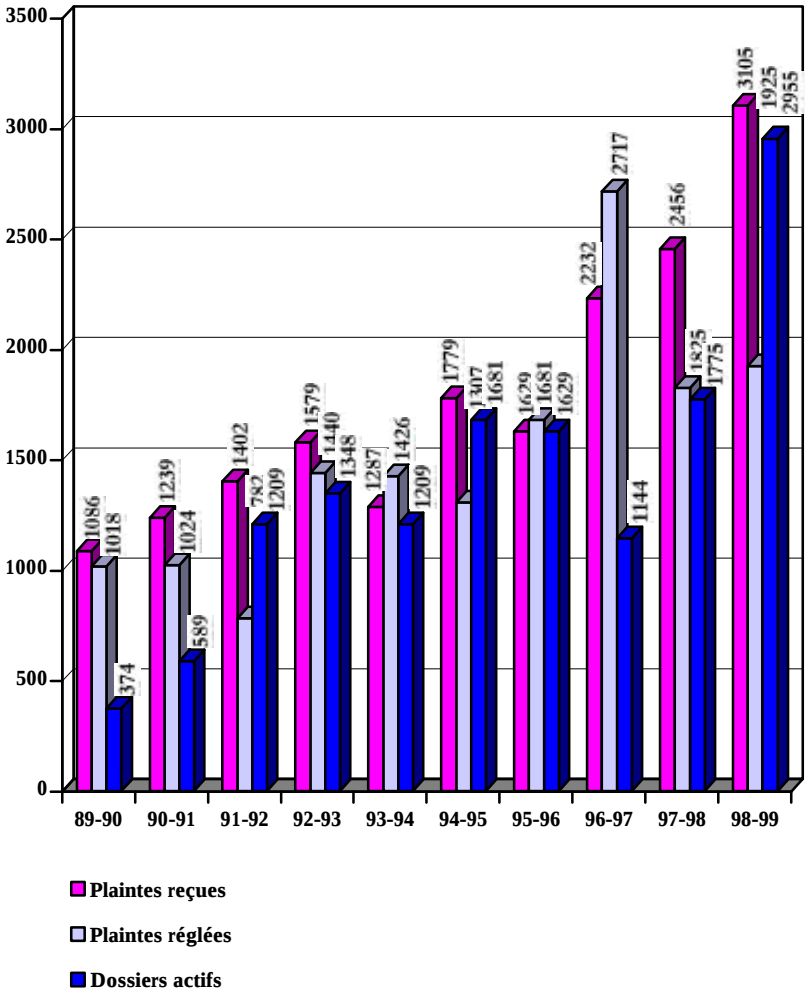
Plaintes réglées par motifs



Plaintes réglées et motifs 1989-1999



Plaintes 1989-1999



* Le tableau reflète des variances minimes apportées aux statistiques pour les années 1996-97 à 1997-98

Mise à jour sur la protection de la vie privée au Canada

Colombie-Britannique

Le commissaire à l'information et à la vie privée de cette province a élaboré cette année une série d'instruments pour aider les organismes à évaluer les effets de nouvelles techniques ou activités et à en atténuer les conséquences négatives sur la vie privée des gens. On peut consulter les documents *Privacy Impact Assessment*, *Personal Information Exchange Agreement*, et *Guidelines for Completing an Information Access Research Agreement between a Public Body and a Researcher* au site Web du commissariat de cette province, à l'adresse www.oipcbc.org.

Au mois de septembre 1998, le commissaire a publié un rapport sur l'échange de renseignements personnels entre les fournisseurs de soins de santé et les services de police sous le régime de la *Freedom of Information and Protection of Privacy Act* de la C.-B. Après la constitution par le gouvernement fédéral du Conseil consultatif sur l'infostructure de la santé, le commissaire de la C.-B. (et certains de ses collègues d'ailleurs au pays) ont abordé devant le Conseil la question de la protection des renseignements médicaux en milieu informatisé.

M. David Flaherty, le premier commissaire à l'information et à la vie privée de la Colombie-Britannique terminera son mandat non renouvelable de six ans le 31 juillet 1999.

Saskatchewan

La législature provinciale a adopté la première loi canadienne en matière de protection des renseignements médicaux le 9 mai 1999. La *Health Information Protection Act* régit les droits individuels et les obligations des «fiduciaires» du système de santé relativement aux renseignements médicaux. La loi est examinée plus en détail à la page 17.

Manitoba

Le Bureau de l'Ombudsman a été désigné comme organisme indépendant d'examen sous le régime de la *Loi sur les renseignements médicaux personnels* (LRMP) et de la *Loi sur l'accès à l'information et la protection de la vie privée*

(LAIPVP). La LAIPVP s'applique à la municipalité de Winnipeg depuis le mois de septembre 1998 et doit entrer en vigueur dans d'autres collectivités locales (œuvrant à l'éducation, à la santé ou au gouvernement local) en 1999. La LRMP s'applique aux personnes qui recueillent ou conservent des renseignements médicaux personnels et qui ont statut de professionnels de la santé (régis par une loi de la législature comme les infirmières, les médecins, les thérapeutes ou désignés par règlement), aux établissements de santé (comme les hôpitaux, les foyers de soins personnels, les laboratoires), aux organismes publics, aux organismes de soins de santé et aux centres de santé communautaire ou aux autres services de soins de santé à vocation communautaire désignés par règlement.

Bien que les enquêtes faisant suite à des plaintes demeurent un pôle de l'activité de la nouvelle Division de l'accès à l'information et de la protection de la vie privée du Bureau de l'Ombudsman, le rôle de cette division s'est élargi pour inclure la vérification, la surveillance, et les activités d'application de la loi.

Au mois de mars 1999, le gouvernement provincial a annoncé la tenue de consultations publiques sur la protection des renseignements personnels dans le secteur privé et a publié un document de travail. Les assemblées publiques devaient avoir lieu en avril et en mai 1999. Le délai prévu pour soumettre des mémoires est le 30 septembre 1999. Le document de travail signale que le projet de loi fédéral C-54, la *Loi sur la protection des renseignements personnels et les documents électroniques* (qui s'appliquera au secteur privé relevant de la compétence fédérale), doit être adopté en 1999.

Québec

Au cours de la dernière année, la Commission d'accès à l'information du Québec (CAIQ) a terminé l'étude :

1) des suites que 22 organismes provinciaux ont données aux 23 recommandations générales et 192 recommandations particulières formulées par la CAIQ au cours des cinq dernières années;

2) des mesures de sécurité prises par les organismes provinciaux pour assurer la confidentialité des renseignements personnels dont ils sont dépositaires.

La CAIQ a déposé deux rapports sur les sujets susmentionnés devant la législature du Québec :

- *Un défi de taille : conjuguer la protection des renseignements personnels et les pratiques administratives*,
- *La sécurité des renseignements personnels dans l'État québécois au printemps 1998 : une démarche bien amorcée*.

Le premier rapport concluait que les recommandations de la CAIQ ont bien peu pesé sur le fonctionnement des organismes provinciaux. Un rapport subséquent indique que plus de la moitié des recommandations ont entraîné des changements.

Le second rapport provenait d'une auto-vérification effectuée par 89 organismes provinciaux. Les résultats indiquent que plus de la moitié des organismes ne donnaient aucune formation à leur personnel sur la méthode appropriée de protéger leurs renseignements personnels. La CAIQ a formulé des recommandations et prévoit effectuer un suivi à l'automne 1999.

Les rapports peuvent être consultés au site Web de la Commission, à l'adresse www.cai.gouv.qc.ca.

…et ailleurs

Directive de l'Union européenne en vigueur

La Directive de l'Union européenne sur la protection des données est entrée en vigueur en octobre 1998. Elle oblige les États membres à faire en sorte que les renseignements personnels concernant des citoyens européens soient protégés lorsqu'ils sont communiqués dans des pays non membres pour y être traités.

Les articles de la Directive traitant de la communication de données personnelles dans des pays étrangers ont soulevé une certaine controverse. Essentiellement, les membres de l'Union européenne ne peuvent transférer de données personnelles concernant des résidents à un État non membre qui n'offre pas de protection « adéquate ». Le Canada répond actuellement à cette description, mais l'adoption prévue du projet de loi C-54 devrait faire de lui l'un des 40 pays qui ont adopté ou sont sur le point d'adopter des lois

pour protéger la vie privée et l'intégrité des données personnelles sur les consommateurs.

Les États-Unis ont résisté à la tendance et élaboré une série de principes refuges pour tenter de satisfaire aux exigences de la Directive. Ces principes ne représentent qu'une tentative d'autoréglementation et imposent une marche à suivre complexe aux consommateurs qui veulent intenter des poursuites contre les contrevenants. L'automne dernier, l'Union européenne a réagi au plan américain en acceptant de ne pas interrompre les flux de données avec les États-Unis pendant les négociations. Pour l'instant, les deux parties n'en sont pas arrivés à un accord, mais les négociations se poursuivent.

Une étude révèle que les employés de première ligne sont mal informés : L'évidence du besoin d'une loi visant la protection des renseignements personnels dans le secteur privé est de plus en plus criante.

Une étude menée récemment par le Centre pour la promotion de l'intérêt public, d'Ottawa, et Action Réseau Consommateur, de Montréal, a porté sur le niveau de connaissance des lois et codes relatifs à la protection des renseignements personnels et au respect de la vie privée chez les employés de première ligne de services que les Canadiens et les Canadiennes utilisent tous les jours : magasins de vente au détail, institutions financières, sociétés de transport et pharmacies. Les conclusions en disent long.

Les chercheurs ont découvert que, même si les entreprises sont assujetties depuis plusieurs années aux lois et aux codes relatifs à la protection des renseignements personnels (dans la province de Québec), les clients obtiennent des réponses différentes au sujet de leurs droits et de la responsabilité de l'entreprise à l'égard des renseignements personnels selon qui fait la demande et sur qui porte celle-ci. L'étude a comparé les réponses fournies à des « clients mystères » à celles qu'ont obtenues des enquêteurs qui se sont identifiés et ont expliqué l'objet des questions. Les employés étaient beaucoup moins précis dans le cas des demandeurs anonymes, dont on pourrait dire qu'ils représentaient le consommateur moyen. L'étude a permis de découvrir un fait non moins troublant, à savoir l'écart considérable entre les différents secteurs en ce qui a trait à la sensibilisation du personnel. Dans L'ensemble, les employés des banques étaient les mieux renseignés, facteur que l'étude a attribué à l'importance et à la permanence de la formation dans ces institutions.

Il est possible d'obtenir des exemplaires de l'étude de 58 pages intitulée *Bilan 1998 sur la protection des renseignements personnels et le respect de la vie privée* auprès des deux organismes précédents.

Sceaux de vie privée sur le Web : moins de protection qu'il ne semble?
La récente vague de mécanismes d'autoréglementation conçus pour encourager les gens à avoir recours au commerce électronique vise moins à protéger leurs renseignements personnels qu'à créer un créneau dans un marché lucratif.

Par exemple, l'Institut canadien des comptables agréés a élaboré *CA WebTrust* qui est supposé protéger les renseignements personnels fournis électroniquement. Le Conseil canadien des bureaux d'éthique commerciale a son sceau *BBBOnline* et, comme nous l'avons signalé dans le rapport de 1997-1998, il y a le sceau de la compagnie TRUSTe. D'autres suivront sans doute.

Le recours par un site Web à un sceau de vie privée soulève plusieurs questions. La plus évidente est sans doute celle de savoir comment un membre du grand public peut déterminer si le sceau résulte ou non d'une évaluation valable des pratiques de l'entreprise en matière de protection des renseignements personnels. Qu'est-ce qui empêche une entreprise non conforme de simplement copier le sceau se trouvant sur le site Web d'une autre entreprise et de l'afficher sur son propre site? La visite des différents sites Web afin de s'assurer que chaque sceau est en vigueur, qu'il n'a pas été révoqué et, le cas échéant, qu'il ne paraît plus sur le site, représenterait une énorme tâche.

Plusieurs raisons incitent à ne pas trop rapidement adopter l'autoréglementation. Il suffit de penser au nombre de violations de la protection des renseignements personnels qui sont survenues sur l'Internet depuis un an. Par exemple, la *Federal Trade Commission* (FTC) américaine a enquête sur plusieurs plaintes alléguant que GeoCities, l'un des sites Web les plus populaires, aurait transmis à des publicitaires du Web des données confidentielles sur ses consommateurs, notamment des enfants. En divulguant ces renseignements, GeoCities a manqué à la promesse de confidentialité qu'il a faite tant aux visiteurs du site qu'à la compagnie TRUSTe, laquelle avait apposé son sceau sur celui-ci. La FTC a déclaré que cette entreprise avait trompé la confiance de ses consommateurs, tant les enfants que les adultes, en ne disant pas la vérité au sujet de l'utilisation des renseignements personnels.

GeoCities est membre de TRUSTe et de la *Online Privacy Alliance*, une coalition d'entreprises et de groupes professionnels qui préconisent l'autoréglementation comme la solution aux préoccupations relatives à la protection des renseignements électroniques. Les incidents sont assurément embarrassants. Comme TRUSTe l'a fait remarquer : «Pour nous, c'est un cauchemar; c'est exactement ce que nous voulons éviter.»[traduction] En août, GeoCities a accepté de régler les accusations de la FTC selon lesquelles l'entreprise a fait une déclaration trompeuse quant au but de la collecte de renseignements personnels auprès des visiteurs du site. Elle a convenu d'afficher un avis clair et en évidence concernant la protection des renseignements personnels et de demander le consentement des parents avant de recueillir de l'information auprès des enfants de 12 ans et moins.

GeoCities n'est pas un cas isolé. Les craintes qu'ont les consommateurs de ne pas être bien protégés sur l'Internet sont fondées. L'an dernier, Yahoo Inc., AT&T Corp. et Nissan Motor Company Ltd. ont semble-t-il laissé des données personnelles non protégées sur leur site ou auraient, par erreur, envoyé par courrier électronique des renseignements personnels à d'autres clients. On a signalé récemment que Microsoft recueillait des données sur des utilisateurs qui avaient expressément demandé l'anonymat. Même le très populaire site Web de la compagnie Air Miles a laissé sans protection environ 50 000 dossiers de clients canadiens. Ces exemples devraient servir à nous rappeler que les entreprises, qu'elles soient grandes ou petites, ne protègent peut-être pas les données personnelles des Canadiens et des Canadiennes aussi bien qu'elles le devraient.

Devant les tribunaux

Robert Lavigne c. le Commissariat aux langues officielles

La Cour fédérale a ordonné au Commissariat aux langues officielles (CLO) de communiquer à M. Lavigne les renseignements personnels qui ont été compilés à son sujet par les employés du CLO pendant leur enquête au sujet d'une plainte relative aux langues officielles.

M. Lavigne avait déposé une plainte au CLO contre Développement des ressources humaines Canada (DRHC). Une fois l'enquête terminée, il a demandé à consulter l'information le concernant dans les déclarations et les notes d'entrevues des témoins figurant dans le dossier. Le CLO avait refusé, en invoquant le fait que la communication de l'information risquerait de « nuire au déroulement d'enquêtes licites » [alinéa 22(1)*b*) de la *Loi sur la protection des renseignements personnels*]. M. Lavigne a porté plainte au Commissaire à la protection de la vie privé, qui est par la suite intervenu dans la poursuite pour appuyer la demande du plaignant.

Dans sa décision rendue le 5 octobre 1998, le juge Dubé a indiqué que le CLO n'était pas tenu à la confidentialité pour s'acquitter du rôle de protecteur du citoyen que lui confère la loi. Il a également conclu que le CLO n'avait pas montré en quoi la communication à M. Lavigne des renseignements personnels le concernant aurait nuit au déroulement de la présente enquête ou d'enquêtes subséquentes. La Cour a également conclu que l'exemption prévue à l'alinéa 22(1)*b*) ne pouvait plus être invoquée une fois l'enquête terminée. Le CLO en a appelé de la décision, et le Commissaire à la protection de la vie privée interviendra à nouveau dans la procédure judiciaire. La date d'audience n'avait pas encore été fixée au moment de l'impression de ces lignes.

Formulaire E-311

La Cour fédérale a aussi appuyé la position du Commissaire à la protection de la vie privée selon laquelle Revenu Canada n'a pas le droit de communiquer l'information figurant sur la Carte de déclaration du voyageur de Douanes Canada (formulaire E-311) à DRHC aux fins du contrôle du programme d'assurance emploi.

Dans une décision rendue le 29 janvier 1999, la juge Tremblay-Lamer a indiqué que la loi n'autorisait pas Revenu Canada à communiquer à la Commission de l'assurance emploi les renseignements personnels apparaissant sur le formulaire E-311. Elle a considéré l'autorisation du ministre du Revenu à cet égard comme une utilisation impropre de son pouvoir discrétionnaire ne correspondant pas à l'objet de la *Loi sur les douanes* et ne tenant pas compte du programme visé. Le gouvernement a fait appel de la décision devant la Cour d'appel fédérale.

Dans une autre affaire, le Commissaire à la protection de la vie privée a appuyé la cause d'un plaignant qui a été portée devant un juge arbitre en vertu de la *Loi sur l'assurance emploi*. Le Commissaire a soutenu que le fait de fouiller tous les voyageurs rentrant au pays sur simple soupçon de fraude de l'assurance emploi enfreint les dispositions de la *Charte canadienne des droits et libertés* visant la « protection contre les fouilles, les perquisitions ou les saisies abusives » et les droits des citoyens de se déplacer en toute liberté. L'affaire a été entendue, mais le jugement n'a pas encore été rendu.

Gestion intégrée

Même s'ils partagent locaux et services administratifs, le Commissariat à la protection de la vie privée et le Commissariat à l'information fonctionnent de façon indépendante en vertu des lois habilitant leurs opérations. Par souci d'économie et d'efficacité pour le gouvernement et les programmes, ces services (finances, personnel, informatique et administration générale) sont centralisés au sein de la direction de la Gestion intégrée. La direction compte un personnel de 14 employés seulement (qui exercent diverses tâches) et un budget représentant environ 14 p. 100 du budget total des dépenses de programme.

Description des ressources

Bien que la gestion innove constamment dans la prestation des services, les ressources en constante diminution des Commissariats amenuisent la capacité de ceux-ci de fournir un niveau de service de qualité au public.

Les ministres du Conseil du Trésor ont pris note des conséquences de ces situations critiques au chapitre des ressources et de la charge de travail lors de leur réunion d'avril 1998. Ils se sont entendus avec les Commissaires sur un examen exhaustif des ressources disponibles (services votés) pendant l'exercice 1998-1999. Le Secrétariat du Conseil du Trésor est en train d'évaluer l'analyse et les recommandations contenues dans le rapport, et vise à faire les rajustements qui s'imposent pendant l'exercice 1999-2000. Les Commissaires prévoient que l'évaluation minutieuse de leurs ressources disponibles, de leurs normes de service et de la prestation des services règlera leurs problèmes financiers et permettra l'amélioration de leurs systèmes d'information désuets.

Le budget combiné que les deux Commissariats avaient projeté pour l'exercice 1998-1999 s'élevait à 8 128 000 $. Les dépenses réelles pour le même exercice étaient de 8 084 150 $. De cette somme, 6 201 525 $ ont été affectés au personnel et 1 019 179 $ ont été versés en services professionnels spéciaux, soit plus de 89 p. 100 de toutes les dépenses. Le solde de 863 446 $ a été affecté à tous les autres coûts, y compris la poste, le téléphone, les télécommunications, les fournitures et l'équipement de bureau. Les dépenses sont ventilées au tableau 1 (Ressources par organismes / activités) et au tableau 2 (Ventilation par type de dépense).

Tableau 1 : Ventilation par organismes / activités

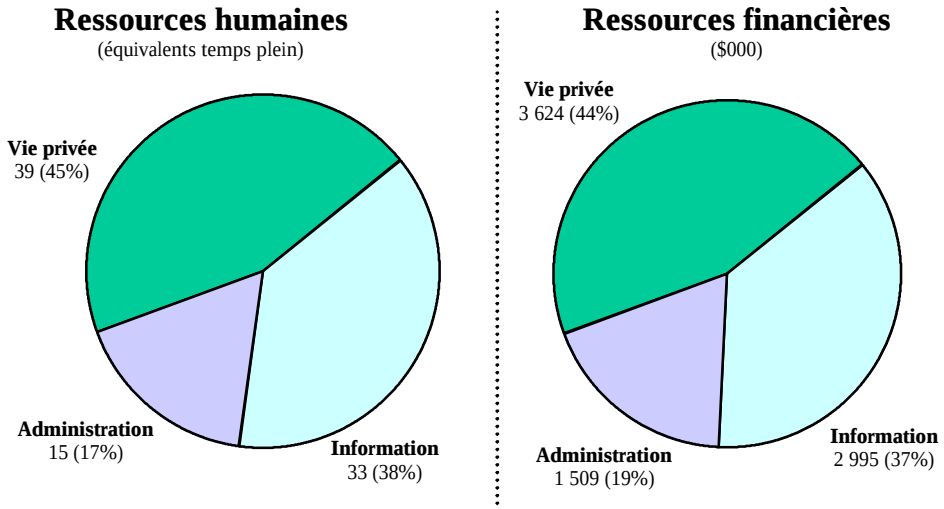
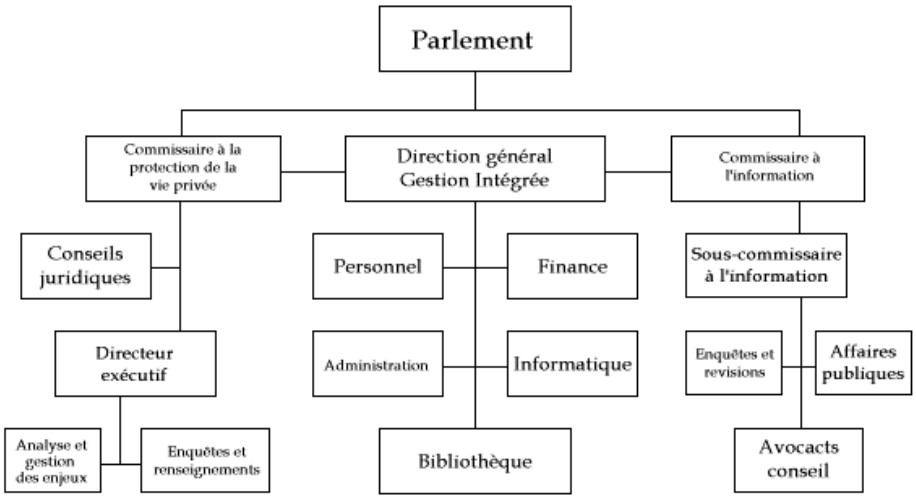


Tableau 2 : Ventilation par article de dépense

	Information	Vie privée	Gestion intégrée	Total
Salaires	2 204 412	2 238 122	705 991	5 148 525
Contributions aux régimes d'avantages sociaux	421 000	491 500	140 500	1 053 000
Transports et communications	37 351	73 844	105 408	216 603
Information	19 330	43 567	3 907	66 804
Services professionnels et spéciaux	207 104	696 583	115 492	1 019 179
Locations	4 593	5 415	19 402	29 410
Achat de services et réparations	738	1 995	27 989	30 722
Services publics approvisionnements fournitures	24 521	18 428	39 693	82 642
Machines et équipements	27 758	58 847	350 287	436 892
Autres paiements	224	106	43	373
Total	**2 947 031**	**3 628 407**	**1 508 712**	**8 084 150**

* Ces dépenses ne reflètent pas les rajustements de fin d'exercice indiqués aux Comptes publics des Commissariats pour 1998-1999.

Organigramme



Guide de la nouvelle loi canadienne sur la protection des renseignements personnels dans le secteur privé

Déjà dans son rapport annuel de 1992-1993, le Commissaire à la protection de la vie privée demandait aux gouvernements de reconnaître que les droits à la vie privée s'appliquent aux secteurs tant public que privé. Faisant état de l'explosion de la technologie informatique, des nouveaux développements dans le domaine de la biotechnologie et les zones grises existant entre le secteur public (doté de lois protégeant la vie privée) et le secteur privé (qui n'en dispose pas), le Commissaire a encouragé le gouvernement fédéral à faire preuve de leadership dans le domaine.

En 1995, le Comité consultatif sur l'autoroute de l'information du Canada a demandé l'adoption d'une loi fédérale souple sur la protection de la vie privée, qui reposerait sur le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation (CSA). À la suite de consultations publiques, le 1er octobre 1998, le gouvernement fédéral a déposé au Parlement le projet de loi C-54 intitulé *Loi sur la protection des renseignements personnels et les documents électroniques*.

La partie 1 de cette loi confère de nouvelles garanties juridiques aux Canadiens lorsque des renseignements personnels sur eux sont utilisés à des fins commerciales. La loi donne suite aux préoccupations grandissantes du public à l'égard de l'utilisation de renseignements personnels par le secteur privé et établit un nouveau cadre national de protection de la vie privée.

La partie 1 aidera aussi le Canada à respecter les nouvelles normes de protection des renseignements établies par l'Union européenne (UE), qui autrement pourrait empêcher les transferts de renseignements vers le Canada. Le Québec est actuellement la seule juridiction en Amérique du Nord à s'être dotée d'une loi sur la protection des renseignements personnels dans le secteur privé qui réponde aux exigences de l'UE.

Les parties 2 à 5 de la loi facilitent l'utilisation par le gouvernement fédéral de ses documents électroniques et établissent le fondement de la reconnaissance juridique des documents et des signatures électroniques. De plus, elles permettront de stimuler la croissance de l'inforoute et d'atteindre l'objectif du gouvernement de faire du Canada un chef de file dans le domaine du commerce électronique d'ici l'an 2000.

Entrée en vigueur et application de la partie 1

La partie 1 entre en vigueur en deux étapes. Dans l'année suivant la promulgation de la loi, cette partie s'appliquera aux sociétés assujetties à la réglementation fédérale, notamment les banques, les compagnies de téléphone, les entreprises de câblodistribution, les radiodiffuseurs et les compagnies de transport interprovincial; le Commissaire fédéral à la protection de la vie privée sera responsable de la surveillance. La partie 1 visera aussi les sociétés d'État non assujetties actuellement à la *Loi sur la protection des renseignements personnels* et à toutes les lois futures du Parlement, à moins d'exemption.

Dans le cadre de cette première étape, la partie 1 visera en outre certaines transactions interprovinciales et internationales, en particulier les baux commerciaux, la vente ou l'échange de listes de clients ou d'autres renseignements personnels.

La deuxième étape commence quatre ans après l'adoption de la partie 1, qui s'étendra alors à tous les organismes assujetties à la législation provinciale, si celle-ci n'offre pas une protection équivalente. Le cas échéant, tout organisme ou activité relevant d'une loi provinciale sera exempté de l'application de la loi fédérale à l'échelle provinciale. La loi fédérale s'appliquera également à toutes les collectes, utilisations et communications de renseignements personnels à l'échelle provinciale et internationale.

Le gouvernement fédéral a déclaré que le Québec ne serait pas touché par la loi fédérale, étant donné que la loi québécoise de 1994 vise l'ensemble du secteur privé et qu'elle ressemble considérablement à la partie 1.

Le Commissaire à la protection de la vie privée collaborera étroitement avec les gouvernements provinciaux et les autres parties intéressées à encourager l'élaboration de lois provinciales harmonisées.

La partie 1 renferme une disposition énonçant la primauté de la nouvelle loi sur toute autre loi fédérale ne stipulant pas le contraire.

Quels types de renseignements seront visés?

La partie 1 s'applique à tout renseignement personnel concernant un individu identifiable, recueilli sous quelque forme que ce soit en rapport avec toute

activité régie par la loi, sous réserve d'exceptions. Les renseignements relatifs au nom, au titre et aux coordonnées des employés ainsi que les renseignements utilisés uniquement à des fins personnelles ou domestiques ne sont pas assujettis à la loi. Sont également exclues certaines catégories de renseignements réglementaires auquel le public a accès. De plus, la partie 1 ne s'applique pas aux renseignements recueillis ou utilisés à des fins journalistiques, artistiques ou littéraires.

Le Code de la CSA : la base de la protection

En vertu de la partie 1, les organisations doivent se conformer au Code de la CSA (dont les principes sont énoncés dans l'annexe 1 de la loi). Le Code, élaboré conjointement par les entreprises, les groupes de consommateurs et le gouvernement, et jugé juste et éclairé, reflète les intérêts légitimes des entreprises et des consommateurs. Le Parlement révisera la loi, y compris l'annexe 1, tous les cinq ans après l'entrée en vigueur de la partie 1.

Droits à la vie privée et obligations des entreprises

Le Code de la CSA établit une norme minimale relative à la protection des renseignements personnels, fondée sur des principes universellement reconnus dans ce domaine. Voici un aperçu des droits à la vie privée et des obligations des entreprises à cet égard en vertu du Code de la CSA et de la partie 1 de la loi. Pour plus de détails, il faut se reporter à la loi.

Responsabilité : Les organisations sont responsables de tous les renseignements personnels qu'elles ont sous leur garde et doivent nommer des personnes qui s'assureront du respect de la loi. Elles doivent aussi mettre en œuvre des politiques et des procédures, former le personnel dans le domaine de la protection des renseignements personnels, ainsi qu'informer le public.

Les organisations demeurent responsables des renseignements lorsqu'elles en confient le traitement à des tierces parties et doivent, par voie contractuelle ou autre, assurer un niveau de protection comparable.

Détermination des fins de la collecte des renseignements : Les organisations doivent documenter les fins auxquelles les renseignements personnels sont recueillis avant de pouvoir s'en servir, y compris l'utilisation de renseignements déjà recueillis pour une nouvelle fin. Idéalement, les fins doivent être précisées aux individus avant la collecte ou au moment de celle-ci, mais toujours avant l'utilisation des renseignements. Les fins doivent

être ce qu'une personne raisonnable estimerait acceptables dans les circonstances.

Consentement : Sauf dans des circonstances limitées et définies, les personnes doivent être informées de toute collecte, utilisation ou communication de renseignements personnels qui les concernent et y consentir. Les organisations peuvent obtenir le consentement après avoir recueilli les renseignements, mais toujours avant de s'en servir. Elles doivent clairement énoncer les fins et faire un effort raisonnable pour s'assurer qu'elles ont été comprises. La nature et la forme du consentement doivent correspondre à la sensibilité des renseignements, aux circonstances et aux attentes raisonnables de la personne. Les organisations ne peuvent exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins indiquées.

Les personnes peuvent retirer leur consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. Les organisations doivent expliquer les conséquences d'un tel retrait.

Dans certains cas, les organisations peuvent recueillir, utiliser ou communiquer des renseignements personnels assujettis à la partie 1 à l'insu de l'intéressé et sans son consentement.

Un renseignement peut être recueilli sans le consentement de l'intéressé si cela est manifestement dans l'intérêt de celui-ci et que son consentement ne peut être obtenu en temps opportun, ainsi que dans des situations précises où l'obtention du consentement pourrait compromettre l'exactitude du renseignement ou l'accès à celui-ci.

Des renseignements déjà recueillis auprès d'une personne peuvent aussi servir à des fins particulières limitées à son insu et sans son consentement. Ces fins, qui incluent les enquêtes sur la violation d'un accord ou de lois, les situations d'urgence mettant en danger la vie par exemple, les recherches ou les études qui ne peuvent être réalisées sans utiliser les renseignements et où il est pratiquement impossible d'obtenir le consentement, ou lorsque les renseignements ont été recueillis sans le consentement comme il a été décrit ci-dessus.

Il existe aussi des circonstances semblables définies où l'organisation ne peut communiquer de renseignement personnel à une tierce partie à l'insu de

l'intéressé et sans son consentement. Il s'agit d'une communication à une institution qui conserve des archives ou à d'autres institutions gouvernementales. Tout renseignement personnel peut être communiqué sans le consentement de l'intéressé si cela se produit cent ans après la collecte du renseignement ou vingt ans après le décès de l'intéressé visé par le renseignement.

Limites de la collecte : Les organisations ne peuvent recueillir que la quantité et le type de renseignements nécessaires aux fins déterminées et doivent procéder de façon honnête et licite.

Limites de l'utilisation, de la communication et de la conservation : Les renseignements personnels ne peuvent être utilisés ou communiqués qu'aux fins pour lesquelles ils ont été recueillis, à moins que la personne concernée n'y consente ou que la loi ne l'exige. Les renseignements personnels ne doivent être conservés qu'aussi longtemps que cela est nécessaire pour réaliser les fins déterminées.

Les organisations devraient élaborer des lignes directrices et mettre en place des procédures pour la conservation des renseignements personnels. Elles devraient détruire, effacer ou dépersonnaliser les renseignements personnels dont elles n'ont plus besoin aux fins déterminées. Des lignes directrices et des procédures officielles doivent régir cette destruction.

Exactitude : Les renseignements personnels utilisés par les organisations doivent être aussi complets, à jour et exacts que l'exigent les fins indiquées, en particulier lorsqu'ils servent à prendre une décision concernant une personne. Les renseignements fournis à des tiers devraient aussi être le plus exacts et le plus à jour possible; il faut préciser clairement les limites se rapportant à l'exactitude et s'assurer qu'elles sont comprises.

Les renseignements personnels ne doivent pas être systématiquement mis à jour, à moins que cela ne soit exigé dans les fins.

Mesures de sécurité : Les renseignements personnels doivent être protégés contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées, au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Au moment de la destruction de renseignements personnels, les organisations doivent veiller à empêcher que des personnes non autorisées n'y aient accès. De plus, elles doivent sensibiliser leurs employés à l'importance de protéger le caractère confidentiel de tous les renseignements personnels.

Transparence : Les organisations doivent fournir au public de l'information générale sur leurs politiques et pratiques concernant la protection des renseignements personnels, y compris le nom et la fonction de la personne responsable du respect de la partie 1, une description générale des genres de renseignements que l'organisation possède et de l'utilisation qu'elle en fait, et la définition de la nature des renseignements communiqués aux organisations connexes telles que les filiales.

Cette information doit être facile à obtenir et compréhensible. Une personne ayant une déficience sensorielle peut demander sur support de substitution de l'information générale ou des renseignements personnels la concernant, si cette information existe déjà sur un tel support ou si le coût de transfert est raisonnable et que la personne en a besoin pour exercer ses droits à la vie privée.

Accès aux renseignements personnels : Les personnes ont le droit d'examiner les renseignements personnels les concernant et d'en contester l'exactitude et l'intégrité. Les organisations doivent indiquer les renseignements personnels qu'elles possèdent, l'usage qu'elles en font et les tiers à qui ils ont été communiqués. Lorsqu'il leur est impossible de fournir une liste des organisations à qui elles ont effectivement communiqué des renseignements, elles doivent fournir une liste des organisations à qui elles pourraient les avoir transmis. Les organisations doivent corriger les renseignements inexacts ou incomplets et, s'il y a lieu, communiquer aux tiers l'information modifiée. Elles doivent noter toute contestation au sujet de modifications à apporter à un dossier et, le cas échéant, en communiquer les détails aux tierces parties concernées.

Sur demande, les organisations doivent aussi aider les personnes à présenter par écrit une demande d'accès. Les renseignements que fournit une personne pour permettre à une organisation de l'informer de l'utilisation qu'elle fait des renseignements recueillis ne doivent servir qu'à cette fin.

Les organisations doivent répondre aux demandes d'accès dans les 30 jours suivant leur réception, à moins d'avoir des motifs raisonnables de proroger le délai. Elles doivent informer les personnes concernées du délai et du droit de celles-ci de porter plainte auprès du commissaire. Faute de donner suite dans le délai prévu, elles sont réputées avoir refusé de répondre à la demande.

Les droits exigés pour avoir accès à des renseignements personnels doivent être directement liés aux frais de photocopie et être raisonnables. Ils peuvent

être imposés seulement si une personne est informée à l'avance du montant approximatif et qu'elle a décidé d'aller de l'avant avec sa demande.

Lorsqu'elle refuse une demande d'accès, l'organisation doit expliquer par écrit ses motifs et les recours dont dispose l'intéressé. Elle doit conserver les renseignements personnels pouvant faire l'objet d'une demande d'accès le temps nécessaire pour permettre aux personnes visées d'épuiser tous les recours à leur disposition en vertu de la partie 1.

La partie 1 énonce aussi des cas particuliers et limités où une organisation peut refuser au demandeur l'accès à des renseignements personnels afin de protéger des renseignements utilisés dans une enquête ou une procédure judiciaire, ou encore les droits à la vie privée de tiers. L'organisation doit informer le commissaire de certains types de refus d'accès aux renseignements.

Plainte à l'égard du non-respect des principes

Les organisations doivent donner suite aux plaintes et aux demandes d'information concernant leurs pratiques de gestion des renseignements personnels et doivent permettre aux personnes de se plaindre du non-respect de la partie 1. Elles doivent mener enquête sur toutes les plaintes et prendre les mesures nécessaires pour remédier aux politiques et aux pratiques déficientes. Les personnes visées doivent être informées des modes de règlement des plaintes, y compris leur droit de s'adresser au Commissaire à la protection de la vie privée.

Dépôt des plaintes auprès du commissaire

Les intéressés peuvent déposer par écrit une plainte auprès du commissaire lorsqu'ils n'ont pas été satisfaits de la façon dont ils ont été traités par une organisation ou s'ils estiment que leur plainte ne peut être réglée autrement. Les plaintes peuvent avoir trait à une violation perçue de la partie 1 de la loi ou d'une exigence ou d'une recommandation du Code de la CSA (annexe 1). Il n'y a pas de délai pour déposer une plainte, sauf si elle se rapporte au refus d'une organisation d'acquiescer à une demande d'accès à des renseignements personnels. Les intéressés doivent normalement déposer leur plainte dans les six mois suivant le refus.

Examen des plaintes

Toutes les plaintes écrites feront l'objet d'une enquête. De plus, si le commissaire a des motifs raisonnables de croire que toute autre question liée à la protection des renseignements personnels devrait être examinée, il peut entreprendre une enquête sans qu'il y ait plainte. Dans tous les cas, l'organisation recevra un avis.

Le commissaire a les pouvoirs d'obtenir et d'examiner tous les renseignements pertinents lorsqu'il mène une enquête. Son Commissariat veille à ce que l'information relative à une enquête demeure confidentielle. Le commissaire peut cependant communiquer des renseignements sur les pratiques de gestion des renseignements personnels d'une organisation si c'est dans l'intérêt public.

Le commissaire ou son délégué peut visiter tout local (autre que résidentiel) occupé par une organisation, à toute heure convenable, examiner et se faire remettre des documents pertinents et s'entretenir en privé avec toute personne sur des éléments utiles à l'enquête. Il peut imposer une amende à l'organisation si celle-ci détruit des renseignements faisant l'objet d'une plainte ou si elle entrave l'enquête.

Le pouvoir le plus important conféré au commissaire est celui de recourir à un mode de règlement des différends tel que la médiation et la conciliation pour régler la plainte. Ces modes mènent généralement au règlement beaucoup plus rapidement, à un coût moindre et de façon beaucoup plus positive que par tout autre moyen.

Dans l'année suivant la réception de la plainte ou le début de l'enquête, le commissaire fait parvenir aux parties intéressées un rapport écrit qui contient ses conclusions et recommandations et les résultats de tout règlement intervenu entre les parties. De plus, il y mentionne l'existence du recours à la disposition du plaignant. Le commissaire peut aussi demander aux organisations de fournir des détails dans un délai déterminé des mesures prises pour la mise en œuvre des recommandations du rapport ou des motifs invoqués pour ne pas proposer de mesures.

Aucun rapport d'enquête n'est exigé dans les cas suivants : les intéressés devraient recourir en premier lieu à d'autres modes de règlement; d'autres lois ou règlements permettraient d'en arriver à une solution plus appropriée; la plainte est futile ou entachée de mauvaise foi; le délai écoulé entre la date où

est survenu l'objet de la plainte et le dépôt de celle-ci. S'il ne produit aucun rapport, le commissaire en informe les deux parties, motifs à l'appui.

Recours devant la Cour fédérale

Le commissaire n'a pas le pouvoir d'obliger les organisations à donner suite aux conclusions ni aux recommandations de son rapport. Dans les 45 jours suivant la réception du rapport, le plaignant ou le commissaire peut demander que la Cour fédérale entende toute question visée par une exigence particulière de la partie 1, y compris certaines exigences du Code de la CSA (mais non les recommandations).

Si un plaignant s'adresse à la Cour, le commissaire peut aussi demander à comparaître au nom du plaignant (avec le consentement de celui-ci) ou comme partie à la procédure.

La Cour peut ordonner à une organisation de revoir ses pratiques de façon à se conformer aux dispositions de la partie 1, notamment d'aviser le public de toute action proposée ou mesure prise pour corriger ses pratiques. Elle peut aussi accorder au plaignant des dommages-intérêts, entre autres en réparation de l'humiliation subie. Il n'existe aucune limite quant au montant des dommages-intérêts exemplaires pouvant être accordé. Lors de l'audition des plaintes, la Cour doit prendre des mesures pour empêcher la communication de renseignements que les organisations ont le droit de ne pas communiquer en vertu de la partie 1.

Vérifications

Le commissaire peut aussi procéder à la vérification des pratiques d'une organisation s'il a des motifs raisonnables de croire que celle-ci n'a pas respecté une obligation de la partie 1 ou qu'elle n'a pas mis en œuvre une recommandation du Code de la CSA. Ces recommandations représentent les meilleures pratiques qui, dans certains cas, peuvent constituer une norme minimale de protection des renseignements personnels selon la sensibilité de l'information, les attentes des personnes visées par les renseignements ou d'autres facteurs.

Aux fins de la vérification, le commissaire dispose des mêmes pouvoirs que lorsqu'il enquête sur une plainte. Tout comme dans les enquêtes, c'est une infraction que de détruire des renseignements personnels qui font l'objet

d'une vérification ou de nuire, de toute autre façon, à la conduite de la vérification.

Une fois la vérification terminée, le commissaire fournira à l'organisation le rapport des conclusions et, s'il y a lieu, des recommandations. Il peut aussi rendre publiques les conclusions des vérifications dans un rapport annuel présenté au Parlement. Bien qu'il ne puisse obliger les organisations à donner suite aux recommandations résultant de la vérification, il peut demander une nouvelle enquête, ce qui entraîne une demande à la Cour fédérale.

Sensibilisation et consultations publiques

Pour sensibiliser le grand public aux questions de la protection de la vie privée et favoriser des normes uniformes dans le domaine de la protection des renseignements personnels, le commissaire peut : mettre en œuvre des programmes d'information; effectuer de la recherche en matière de protection de la vie privée; et encourager le secteur privé à élaborer et à mettre en œuvre des politiques et des codes de pratiques, fondés sur la partie 1 et le Code de la CSA.

Le commissaire a aussi le pouvoir de consulter les commissaires provinciaux à la protection de la vie privée ou autres parties et de conclure des accords afin de coordonner, s'il y a lieu, l'activité liée à l'instruction des plaintes. Il peut aussi signer des ententes avec les provinces afin de faire des recherches liées à la protection de la vie privée et d'en publier les résultats, ainsi que d'élaborer des contrats types portant sur la protection des renseignements personnels d'une province à l'autre ou d'un pays à l'autre. Ces contrats peuvent contribuer grandement à l'uniformisation des normes dans ce domaine et au respect des exigences internationales liées à la protection de la vie privée.

Le commissaire doit aussi déposer devant le Parlement un rapport annuel sur toutes les activités relatives à la partie 1, y compris la situation concernant la législation provinciale sur la protection de la vie privée et d'autres sujets concernant la protection des renseignements personnels sur la scène interprovinciale et internationale.

Protection du dénonciateur

La partie 1 protège les employeurs ou d'autres personnes contre des récriminations pour avoir agi de bonne foi et en se fondant sur des motifs

raisonnables afin de faire observer les dispositions de la partie 1 ou pour avoir informé le commissaire des infractions perçues. Ces personnes peuvent demander que leur identité soit gardée confidentielle lorsqu'elles s'adressent au commissaire. Ce dernier est obligé d'assurer l'anonymat en toutes circonstances.

Les employeurs ne peuvent sévir d'aucune façon contre un employé ou un travailleur autonome qui, selon eux, a informé, en se fondant sur des motifs raisonnables, le commissaire au sujet d'une infraction réelle ou possible de la partie 1, a accompli un acte pour empêcher ce qu'il perçoit comme une contravention, fait part de son intention d'agir ainsi ou a refusé ou fait part de son intention de refuser d'exécuter des tâches qui constitueraient une contravention à la loi.