



Rapport annuel au Parlement 2000-2001





Rapport annuel au Parlement 2000-2001



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

(613) 995-8210, 1-800-282-1376
Télec. (613) 947-6850
ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 2001
N° de cat. IP30-1/2001
ISBN 0-662-66226-1

Cette publication est également disponible sur notre site Web à www.privcom.gc.ca

**Office of the
Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissariat
à la protection de
la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



Décembre 2001

L'honorable Daniel Hays
Président
Sénat du Canada

Monsieur,

J'ai l'honneur de remettre au Parlement mon rapport annuel pour les périodes du 1^{er} avril 2000 au 31 mars 2001 dans le cas de la *Loi sur la protection des renseignements personnels* et du 1^{er} janvier 2001 au 30 novembre 2001 dans le cas de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Le moment de la parution du rapport de cette année est exceptionnel. J'avais décidé de remettre mon rapport au début de l'automne cette année plutôt qu'au printemps comme d'habitude, pour deux raisons : tout d'abord, étant entré en fonction en septembre 2000, je voulais une période suffisante d'expérience sur laquelle fonder mon rapport; et, en second lieu, vu que la *Loi sur la protection des renseignements personnels et les documents électroniques* est entrée en vigueur le 1^{er} janvier 2001, je préférais que le rapport fasse état d'une expérience suffisante de la nouvelle loi. Puis, les événements du 11 septembre, et les questions de protection des renseignements personnels qu'ils ont soulevées, m'ont obligé à attendre jusqu'à maintenant. Le Commissariat reviendra à son échéancier normal avec un rapport le printemps prochain.

Veuillez agréer, Monsieur, l'expression de mes sentiments les meilleurs.

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

A handwritten signature in black ink, appearing to be 'G. Radwanski', written in a cursive style.

George Radwanski

**Office of the
Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissariat
à la protection de
la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



Décembre 2001

L'honorable Peter Milliken
Président
Chambre des communes

Monsieur,

J'ai l'honneur de remettre au Parlement mon rapport annuel pour les périodes du 1^{er} avril 2000 au 31 mars 2001 dans le cas de la *Loi sur la protection des renseignements personnels* et du 1^{er} janvier 2001 au 30 novembre 2001 dans le cas de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Le moment de la parution du rapport de cette année est exceptionnel. J'avais décidé de remettre mon rapport au début de l'automne cette année plutôt qu'au printemps comme d'habitude, pour deux raisons : tout d'abord, étant entré en fonction en septembre 2000, je voulais une période suffisante d'expérience sur laquelle fonder mon rapport; et, en second lieu, vu que la *Loi sur la protection des renseignements personnels et les documents électroniques* est entrée en vigueur le 1^{er} janvier 2001, je préférais que le rapport fasse état d'une expérience suffisante de la nouvelle loi. Puis, les événements du 11 septembre, et les questions de protection des renseignements personnels qu'ils ont soulevées, m'ont obligé à attendre jusqu'à maintenant. Le Commissariat reviendra à son échéancier normal avec un rapport le printemps prochain.

Veuillez agréer, Monsieur, l'expression de mes sentiments les meilleurs.

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

A handwritten signature in black ink, appearing to be 'G. Radwanski'.

George Radwanski



TABLE DES MATIÈRES

Compte rendu sommaire du Commissaire	I
Première partie – Rapport concernant la <i>Loi sur la protection des renseignements personnels</i>	29
Introduction	29
Enquêtes	30
Plaintes en vertu de la <i>Loi sur la protection des renseignements personnels</i>	30
Définitions aux termes de la <i>Loi sur la protection des renseignements personnels</i>	34
Sommaire de cas choisis en vertu de la <i>Loi sur la protection des renseignements personnels</i>	35
<i>Des renseignements personnels trouvés dans un conteneur à ordures au MDN</i>	35
<i>Des renseignements personnels détruits de façon prématurée à DRHC</i>	36
<i>Statistique Canada : préoccupations concernant la publication de renseignements sur certains groupes</i>	37
<i>Un nouveau système électronique à la Défense nationale a compromis la vie privée de milliers de personnes</i>	39
<i>Santé Canada ne sait pas si elle a communiqué des renseignements personnels</i>	40
<i>Des renseignements sur des permis de petite embarcation utilisés pour évaluer les taxes de vente</i>	41
<i>Absence de normes touchant la communication de renseignements personnels aux médecins</i>	41
<i>Les renseignements personnels d'un revendicateur du statut de réfugié communiqués à un autre revendicateur</i>	43
<i>Jurys de sélection et notes manuscrites</i>	44
<i>Le courrier électronique personnel n'est pas nécessairement privé</i>	44
Incidents visés par la <i>Loi sur la protection des renseignements personnels</i>	47
<i>L'ouverture du courrier – le droit à la vie privée doit être la première considération</i>	47
<i>Santé Canada et sa liste de présumés utilisateurs de marijuana</i>	48
<i>Vol de demandes remplies de permis d'armes à feu à Justice Canada</i>	49
<i>Des préoccupations au sujet d'une technologie d'identification biométrique</i>	50

<i>Une contribuable a reçu le remboursement d'une autre personne</i>	50
Communications dans l'intérêt public	51
Pratiques en matière de vie privée et examens	60
Introduction	60
<i>Des renseignements personnels n'ayant pas été déchiquetés –</i> <i>Golden West Document Shredding, Inc.</i>	61
<i>Préoccupations en matière de vie privée du Programme canadien des armes à feu</i>	65
<i>Un nouveau protocole relatif aux bases de données est adopté suivant</i> <i>le Fichier longitudinal sur la main-d'œuvre</i>	68
Examens	70
<i>La Commission de l'immigration et du statut de réfugié et</i> <i>la Commission canadienne de sûreté nucléaire</i>	70
Devant les tribunaux	70
Introduction	70
Décisions récentes	71
<i>Le Commissaire à la protection de la vie privée c. le Conseil canadien</i> <i>des relations de travail</i>	71
<i>Le Commissaire à l'information du Canada (appelant) c. le Commissaire de</i> <i>la GRC (intimé) et le Commissaire à la protection de la vie privée (intervenant)</i>	72
Affaires en instance	73
<i>Formulaires de déclaration du voyageur (E-311)</i>	73
<i>Le Commissaire à la protection de la vie privée c. le Procureur général du Canada</i>	73
<i>Contestation en vertu de la Charte</i>	74
<i>Clayton Charles Ruby c. le Solliciteur général</i>	76
<i>Le Commissariat aux langues officielles (appelant) c. Robert Lavigne (intimé)</i>	77
Deuxième partie – Rapport concernant la Loi sur la protection des renseignements <i>personnels et les documents électroniques</i>	79
Introduction	79
Mise à jour des lois provinciales et territoriales	81
Détermination d'« essentiellement similaire »	81
Consentement	81
Critère de la personne raisonnable	82
Droits d'accès et de correction	82
Surveillance	82

Voies de recours	82
Initiatives législatives en vue de réglementer le secteur privé	82
Secteur de la santé	83
Loi pour le secteur privé	83
Enquêtes	83
Les Conclusions du Commissaire	84
<i>Activités de surveillance vidéo dans un endroit public</i> [principe énoncé à l'article 4.3 de l'annexe 1]	85
<i>Messages électroniques non sollicités d'un fournisseur de services Internet</i> [principe énoncé à l'article 4.3 de l'annexe 1]	86
<i>Le Commissaire étudie le domaine de compétence dans une affaire</i> <i>de communication de renseignements d'une filiale bancaire à un tiers [article 30] . .</i>	87
<i>Une cliente d'une banque demande des renseignements sur sa cote de crédit</i> [principe énoncé à l'article 4.9 de l'annexe 1, et article 8]	88
<i>Conservation de renseignements personnels après le rejet d'une demande</i> [principe énoncé à l'article 4.5 de l'annexe 1]	89
<i>Sûreté du service téléphonique automatisé d'une banque</i> [principe énoncé à l'article 4.7 de l'annexe 1]	90
<i>Un musicien s'oppose à ce qu'une organisation professionnelle recueille</i> <i>des renseignements sur son salaire [article 2]</i>	92
<i>Utilisation et communication de renseignements personnels dans</i> <i>les annuaires téléphoniques [principe énoncé à l'article 4.3 de l'annexe 1]</i>	93
<i>Inscription du numéro de compte sur un chèque à la banque [paragraphe 5(3)]</i>	94
<i>Une entreprise de camionnage recueille des renseignements personnels</i> <i>prévus pour Douanes Canada [principe énoncé à l'article 4.4 de l'annexe 1]</i>	96
<i>Une banque perd des renseignements personnels concernant une cliente</i> [principe énoncé à l'article 4.7 de l'annexe 1, et paragraphe 12(2)]	97
<i>Un demandeur de carte de crédit s'oppose à la politique sur l'échange</i> <i>de renseignements d'une banque</i>	98
<i>Une banque accusée de retenir des certificats d'obligation</i> [principe énoncé à l'article 4.9 de l'annexe 1, et article 8]	99
<i>Vente de renseignements sur les habitudes de prescription des médecins [articles 2 et 3] . .</i>	100
<i>Obstacles à la démarche d'un exécuteur testamentaire tâchant d'obtenir</i> <i>des renseignements concernant un coffre bancaire [principes énoncés aux</i> <i>articles 4.5 et 4.9 de l'annexe 1, et paragraphe 8(7)]</i>	102
<i>Un employé prétend que son employeur a communiqué sans son consentement</i> <i>des renseignements à une société de placement [paragraphe 7(3) et</i> <i>principes énoncés aux articles 4.3 et 4.5 de l'annexe 1].</i>	103

<i>Un demandeur affirme ne pas avoir reçu son rapport de solvabilité d'une agence d'évaluation [article 8].</i>	104
<i>Une entreprise de transport aérien accusée de priver des voyageurs de leur droit de consulter des renseignements personnels au sujet d'incidents de voyage [principes énoncés aux articles 4.1 et 4.9 de l'annexe 1]</i>	105
<i>Une employée s'oppose à ce que son employeur inscrive son numéro de compte bancaire sur sa fiche de paie [principes énoncés aux articles 4.3 et 4.7 de l'annexe 1]</i>	107
<i>Une entreprise demande le NAS d'une cliente en vertu d'une politique [principes énoncés aux articles 4.3.3 et 4.4.1 de l'annexe 1, et paragraphe 5(3)]</i>	109
<i>Une utilisatrice accuse un FSI de lire ses messages électroniques et d'empêcher leur transmission [principe énoncé à l'article 4.3 de l'annexe 1].</i>	110
<i>Un employeur envoie à des tiers des copies d'une réponse à des demandes d'accès présentées par une employée [principes énoncés aux articles 4.3 et 4.5 de l'annexe 1, et paragraphe 5(3)]</i>	112
<i>Une entreprise de téléphone demande des pièces d'identité aux nouveaux abonnés [principes énoncés aux articles 4.2 et 4.2.3 et aux articles 4.3, 4.3.2 et 4.3.3 de l'annexe 1, et paragraphe 5(3)]</i>	114
<i>Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web [article 2, et principe énoncé à l'article 4.3 de l'annexe 1].</i>	116
<i>Un couple prétend que la banque lui a refusé l'accès à des renseignements sur une demande de prêt [paragraphe 8(3) et 8(5)].</i>	117
Incidents en vertu de la LPRPDÉ.	119
<i>Une entreprise de transport recueille et communique des renseignements personnels concernant les passagers</i>	119
<i>Un site Web diffuse des conversations par téléphones cellulaires</i>	120
Pratiques et examens en matière de vie privée.	122
Devant les tribunaux	122
<i>Mathew Englander c. Telus Communications Inc</i>	122
<i>Ronald G. Maheu c. le Procureur général du Canada et IMS Health Canada</i>	123
Communications et sensibilisation du public.	124
Documents de sensibilisation du public	125
Publicité.	125
Site Web	125
Troisième partie – Services de gestion	127
Préparatifs pour la mise en œuvre de la loi pour le secteur privé.	127
Structure organisationnelle	130



COMPTE RENDU SOMMAIRE DU COMMISSAIRE

Il s'agit de mon premier rapport à l'intention des Canadiens et Canadiennes à titre de Commissaire à la protection de la vie privée et je profite de l'occasion qui m'est offerte pour porter un regard en arrière et faire le bilan des réalisations de l'an dernier. En peu de temps, nous avons été témoins d'événements extraordinaires, à la fois technologiques et sociaux, qui ont comporté une incidence sans précédent sur la vie privée. Et, en ce qui me concerne personnellement, j'ai vécu une année remarquable remplie de découvertes.

Je me réjouis qu'au cours de la brève durée de mon mandat, plusieurs importantes victoires ont été remportées concernant les droits à la vie privée des Canadiens et Canadiennes :

- Le projet de loi antiterroriste du gouvernement fédéral a été modifiée de façon à assurer qu'il fait obstacle aux droits à la vie privée seulement lorsque cela est absolument nécessaire afin d'atteindre les objectifs

légitimes en matière de sécurité. Dans sa version initiale, la Loi renfermait des dispositions qui dépassaient largement les objectifs fixés. Suivant ces dispositions, le Procureur général aurait été autorisé à retirer aux Canadiens et Canadiennes toute protection de la vie privée, dans la mesure où il l'aurait jugé indiqué, en délivrant des certificats globaux qui auraient abrogé la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. La ministre de la Justice a reconnu le bien-fondé de mes observations et a apporté des modifications qui ont tenu pleinement compte de mes réserves.

- L'ouverture du courrier en provenance de l'étranger par les agents de l'Agence des douanes et du revenu du Canada, pour le compte de Citoyenneté et Immigration Canada, a été limitée de façon à respecter davantage les droits à la vie privée. Cette ancienne pratique, fondée sur une distinction arbitraire et périmée entre le courrier et les colis en fonction du poids, énoncée dans la *Loi sur les douanes*, était parfaitement légale, tout en étant profondément viciée d'un point de vue de



George Radwanski
Commissaire à la protection
de la vie privée du Canada

la vie privée. L'envoi du courrier dans de grandes enveloppes, comme l'exigent les services de messagerie prioritaire, faisait qu'il était suffisamment lourd pour ne plus être visé par l'exemption, qui consistait à protéger le courrier des Canadiens et Canadiennes de toute ouverture en l'absence d'un mandat. Suite à des discussions avec le ministre du Revenu national, ce dernier a fait en sorte que l'Agence révise ses procédures afin de respecter l'esprit de la loi. Lorsqu'on détermine le poids du courrier, on ne tient plus compte des enveloppes extérieures pour distinguer entre le courrier visé par les mesures de protection des renseignements personnels et les colis.

- On n'a pas donné suite à un projet de loi provincial profondément vicié sur la protection des renseignements personnels sur la santé en Ontario, qui aurait donné carte blanche au gouvernement provincial pour violer les droits à la vie privée en matière de santé. Parce que notre droit à la vie privée est indivisible – c'est-à-dire qu'il ne peut être respecté au fédéral et violé au provincial – j'ai accepté l'invitation de témoigner au sujet du projet de loi devant un comité de l'Assemblée législative. À l'encontre d'autres témoins qui ont recommandé des amendements, j'ai suggéré de retirer le projet de loi et de revenir à la case départ parce que la démarche qu'il proposait était fondamentalement défectueuse.

Le projet de loi est resté en plan au Feuilleton. J'ai bon espoir que son substitut éventuel protégera réellement la vie privée.

Ces développements me portent à croire que la structure juridique canadienne en matière de vie privée, qui comprend un haut fonctionnaire du Parlement ou un ombudsman dont le mandat est de surveiller les droits à la vie privée des Canadiens et Canadiennes, est fondée et efficace. Avec le soutien suffisant du public, que l'on peut s'assurer en présentant les faits avec à-propos et persuasion, de grandes choses peuvent être réalisées et bon nombre de préjudices écartés.

J'ai assumé cette charge avec la détermination d'être un champion de la protection du droit à la vie privée de tous les Canadiens et de toutes les Canadiennes. Pour ce faire, j'ai cru bon de revigorer le Commissariat à la protection de la vie privée et de sensibiliser davantage les Canadiens et Canadiennes aux questions touchant la vie privée qui ont une incidence sur leur vie.

Par conséquent, l'effectif du Commissariat a presque doublé depuis l'an dernier. Lorsque je suis entré en fonction en septembre 2000, celui-ci comptait 54 employés. Au 30 novembre 2001, le personnel s'était accru et totalisait 84 (97 si l'on comprend la Direction générale des services de gestion intégrée). Cet accroissement visait deux objectifs : nous acquitter de nos nouvelles responsabilités de surveillance aux termes de la *Loi sur la protection des*

LA VIE PRIVÉE EST MENACÉE COMME ELLE NE L' A JAMAIS ÉTÉ AUPARAVANT.



renseignements personnels et les documents électroniques, qui est entrée en vigueur en janvier; et créer la direction des communications qui joue un rôle clé en vue de sensibiliser davantage au droit fondamental à la vie privée.

La conscientisation du public est une composante indispensable du rôle que je suis appelé à jouer. En tant qu'ombudsman, je dispose de deux mécanismes fondamentaux : la persuasion et la publicité. Il est bien évident que la persuasion est grandement rehaussée si elle est appuyée, dans la mesure du possible, d'une opinion publique avertie et alerte.

Les Canadiens et Canadiennes doivent connaître et comprendre leurs droits à la vie privée et exiger que ceux-ci soient pleinement respectés. C'est pourquoi, depuis mon entrée en fonction, j'ai accordé une importance primordiale à mes responsabilités de communicateur. Jusqu'à date, j'ai prononcé 35 discours à divers auditoires partout au Canada, et accordé plus de 210 entrevues aux médias.

Bien entendu, avant d'être nommé, j'étais sensibilisé au fait que la vie privée constitue un enjeu important. J'étais conscient qu'il s'agissait d'un élément essentiel d'une société libre, et j'ai convenu avec l'ancien juge LaForest de la Cour suprême que la vie privée se trouvait « au cœur de la liberté dans un État moderne ». [traduction libre] Et le postulat, à savoir que la vie privée est le droit le plus fondamental duquel émanent toutes les libertés – la liberté de parole, la liberté

d'association, la liberté de choix, pour ne nommer que celles-là –, m'a frappé en raison de sa justesse.

Mais je me suis vite rendu compte dans l'exercice de ma charge que la vie privée était encore beaucoup plus importante, et sa protection plus urgente, que ce que j'avais escompté.

Il s'agit d'une période critique en tant que Commissaire à la protection de la vie privée. La vie privée est menacée comme elle ne l'a jamais été auparavant. Par le passé, on a souvent sonné le glas de la vie privée. Mais il est triste de dire que ce son d'alarme a été rejeté par de nombreuses personnes parce qu'elles y voyaient une exagération.

Aujourd'hui, une personne assez bien informée ne peut plus se permettre de le rejeter. Les moyens technologiques qui peuvent supprimer la vie privée sont en place, et pas seulement les ordinateurs et la technologie de traitement des renseignements, mais aussi la panoplie de sorcelleries technologiques allant des caméras vidéo, aux logiciels de reconnaissance de visage et aux cartes d'identité « intelligentes ». Et les motifs pour le faire existent bel et bien, et il ne s'agit pas nécessairement de motifs ignobles. En effet, les plus grandes menaces à la vie privée ne sont souvent pas posées par les personnes qui veulent y porter atteinte, mais bien par celles qui soutiennent avec la plus grande conviction que la vie privée doit être sacrifiée à quelque bien plus important.

Bon nombre d'entre nous pouvons maintenant envisager un monde sans vie privée, pas seulement l'envisager, mais aussi le présager comme probable et imminent, dans un avenir que nous verrons. Nous n'avons pas besoin d'un George Orwell pour nous dire « Tâchez d'imaginer ce qu'il en serait ». [traduction libre] Nous commençons tous à le voir autour de nous.

Nous faisons maintenant face à la possibilité réelle de devoir vivre en surveillant nos arrières, soit métaphoriquement, soit littéralement. Nous pouvons tous envisager une situation réelle et imminente dans laquelle il nous faudra peser chaque geste, chaque transaction, chaque déclaration, voire chaque contact humain, en pensant à qui en prendra connaissance, les jugera, les interprétera faussement ou les utilisera à notre détriment.

Est-ce là la liberté? Bien au contraire, il s'agit d'une réalité propre aux sociétés totalitaires.

Pourtant, je m'inquiète à l'idée que de nombreux Canadiens et Canadiennes soient au courant de l'atteinte à leur vie privée sans toutefois se rendre compte de son ampleur. Ils y portent attention seulement lorsque leur propre vie privée a été violée, lorsqu'il est déjà trop tard. Une fois que la vie privée a été violée, celle-ci ne peut jamais être pleinement rétablie. Lorsque les renseignements personnels de l'un d'entre nous sont révélés à une personne qui n'a pas affaire à les connaître, il est impossible de faire que cela soit autrement.

Les pressions exercées sur les droits à la vie privé ont de toute évidence été accusées dans la foulée des attaques terroristes du 11 septembre. Lorsque règne un climat de peur et d'incertitude, il devient facile de croire que plus l'État détient de renseignements à notre sujet, plus en sécurité nous serons. Cela, en retour, peut conférer une nouvelle légitimité injustifiée à ce qui pose justement les plus grandes menaces à la vie privée, par exemple, la prolifération de la surveillance vidéo, l'utilisation généralisée de la technologie de reconnaissance biométrique ou les cartes d'identité nationales.

Ces pressions s'intensifient parce qu'un climat de crainte fraye la voie non seulement aux intrusions dans la vie privée, mais tend également à décourager ou à sanctionner la dissidence. À la lumière de la destruction semée par les terroristes, quiconque s'oppose aux mesures qui même semblent vaguement rehausser la sécurité, doit accepter de courir le risque d'être accusé d'irresponsabilité.

Pourtant, le monde a toujours été un endroit dangereux, et l'évolution des droits fondamentaux, comme le droit à vie privée, nous enseigne que leur plus grande valeur découle de leur pérennité et de leur capacité de nous protéger en période d'adversité. Lorsqu'il n'y a pas de raison contraignante de violer un droit, nous le percevons non en tant que droit mais comme un fait de la vie. C'est seulement lorsque nous voulons poursuivre un but que

SI NOUS RÉAGISSONS AU TERRORISME EN NOUS PRIVANT DE FAÇON EXCESSIVE ET INUTILEMENT DE NOTRE DROIT À LA VIE PRIVÉE ET DES LIBERTÉS QUI EN DÉCOULENT, LE TERRORISME AURA ALORS REMPORTÉ UNE GRANDE ET TERRIBLE VICTOIRE.

nous estimons irrésistible en faisant fi de toute autre considération, que l'engagement de notre société à la protection des droits fondamentaux est vraiment mis à l'épreuve.

La vie privée et les autres libertés et valeurs précieuses qui définissent la société canadienne ne sont pas des frivolités ou des luxes dans la situation que nous vivons depuis le 11 septembre. Plutôt, ce sont les enjeux les plus importants dans une telle situation. Si nous réagissons au terrorisme en nous privant de façon excessive et inutilement de notre droit à la vie privée et des libertés qui en découlent, le terrorisme aura alors remporté une grande et terrible victoire.

Au dire de tous, l'objet visé par la campagne terroriste maintenant en cours est d'attaquer et de miner la nature même de la société américaine et, partant, de toutes les sociétés démocratiques. Cela fait que nos libertés et valeurs, et surtout la vie privée, sont les plus importantes cibles. Toute restriction inconsidérée de ces libertés et toute atteinte déplacée à la vie privée, au lieu d'accroître notre sentiment de sécurité, montreraient que le terrorisme atteint ses objectifs et présente une occasion de fomenter la terreur.

Mon rôle à titre de Commissaire à la protection de la vie privée est de faire tout en mon pouvoir pour assurer que le droit humain et la valeur canadienne fondamentale, la vie privée, ne succombent pas au terrorisme.

En m'acquittant de cette responsabilité, je ne soutiens pas que le droit à la vie privée est un droit absolu ou encore que certaines mesures intrusives ne sont pas nécessaires en réponse aux menaces à la sécurité auxquelles nous faisons maintenant face.

Il reste qu'il est de mon devoir d'insister pour que nous décidions toujours de telles mesures avec calme, circonspection et au cas par cas, et que celles-ci doivent être justifiées suivant des critères clairs. J'ai recommandé les critères suivants à la fois pour les gouvernements et le secteur privé :

- Toute mesure proposée pour limiter le droit à la vie privée ou empiéter sur celui-ci doit être nécessaire afin d'aborder un problème particulier.
- La mesure doit être efficace pour régler le problème, autrement dit, il doit être démontré que celle-ci accroîtra le niveau de sécurité et non seulement notre sentiment de sécurité.
- Le degré d'intrusion dans la vie privée et de limitation de celle-ci doit être proportionnel à l'avantage en matière de sécurité qui en découlera. Autrement dit, il ne faut pas utiliser un marteau pour tuer un moustique.
- Enfin, il ne peut y avoir de mesures moins intrusives qui permettraient d'atteindre les mêmes résultats.

Bien que certaines difficultés initiales aient été éprouvées, la réponse législative du gouvernement fédéral à la menace de terrorisme satisfait aux critères énoncés ci-dessus concernant les droits à la vie privée. Je crois que cette réponse a permis d'établir un équilibre raisonnable et prudent entre la sécurité et la vie privée. Je continue à mettre de l'avant mes réserves et recommandations quant aux mesures législatives à venir.

Au cours des prochains mois, il ne fait aucun doute que d'autres difficultés et menaces relatives à la vie privée se présenteront dans la foulée des événements du 11 septembre. Les choix que nous ferons revêtiront une importance considérable.

Au cours des jours et des semaines qui ont suivi les attaques, le public a pris connaissance des questions qui inquiétaient depuis longtemps les défenseurs des droits à la vie privée. Il s'est rendu compte que de vastes intérêts industriels sont impatients de fabriquer et de vendre la technologie de surveillance : les caméras vidéo, les systèmes de reconnaissance de visage, les lecteurs d'empreintes digitales, les dispositifs de surveillance du courrier électronique et de sites Web, les cartes d'identité « intelligentes », et les systèmes de repérage. Et il a vu qu'un grand nombre de personnes sont prêtes à soutenir que quiconque n'a rien à cacher à son sujet ne devrait pas s'opposer à tout révéler.

Depuis l'an dernier, bien avant les tragiques événements du 11 septembre, je me suis rendu à l'évidence que la vie privée serait une question déterminante de la nouvelle décennie. C'est un message que j'ai maintes fois répété au cours de mes communications publiques. Jusqu'à récemment, ce que je voulais dire, c'est que nous faisons face à des choix sans précédent et irrévocables touchant la vie privée en raison des percées technologiques et scientifiques, et que ces choix détermineront la qualité de notre vie.

Cela demeure vrai, mais maintenant plus que jamais, la vie privée sera une question décisive parce que les décisions que nous prendrons concernant l'équilibre entre la sécurité et la vie privée détermineront le genre de société que nous léguerons à nos enfants et à nos petits enfants. Même une société orwellienne exempte de vie privée ne serait entièrement sûre – même un État policier le plus tyrannique qui soit n'est pas à l'abri du terrorisme – mais le fait de nous désinvestir graduellement de nos droits à la vie privée dans l'intérêt de la sécurité éliminerait en retour de notre vie la dignité et la liberté qui sont les gages de notre société.

En rétrospective, nous verrons inévitablement cette décennie comme celle où nous avons eu l'occasion d'affirmer la valeur cruciale de la vie privée et de la défendre contre ses assaillants. J'espère fermement que nous serons capables de nous souvenir de cette décennie comme de celle où nous avons saisi cette occasion et franchi un pas décisif.

JE PRÉFÈRE TOUTEFOIS UNE DÉFINITION PLUS MODERNE ET PEAUFINÉE DE LA VIE PRIVÉE EN TANT QUE DROIT D'EXERCER UN CONTRÔLE SUR L'ACCÈS À SES RENSEIGNEMENTS PERSONNELS AINSI QU'À SA PERSONNE.

Autrefois, la majorité des personnes définissaient la vie privée en employant une variante de la célèbre formule de Samuel Warren et de Louis D. Brandeis, comme « le droit de ne pas être dérangé ». [traduciton libre] Il s'agit toujours d'une définition valable et elle reflète assurément l'importance viscérale que les gens accordent à la vie privée.

Je préfère toutefois une définition plus moderne et peaufinée de la vie privée en tant que droit d'exercer un contrôle sur l'accès à ses renseignements personnels ainsi qu'à sa personne. Cette définition permet de mieux saisir la nature des menaces modernes posées à la vie privée, qui se présentent surtout dans le contexte de la collecte et de l'utilisation des renseignements à notre sujet.

C'est pourquoi j'ai dit si souvent au cours de l'année dernière que nous sommes à la croisée des chemins. Ce que je veux dire, c'est que les moyens que nous avons pris pour protéger la vie privée par le passé, plutôt les moyens qui permettaient d'assurer sa protection sans que nous nous en occupions, ne sont plus aussi efficaces et ils le seront de moins en moins avec le temps.

Déjà la protection de la vie privée était plus ou moins assurée « par défaut ». Lorsque les dossiers imprimés qui renfermaient des renseignements nous concernant étaient éparpillés à de nombreux endroits, la constitution d'un dossier détaillé sur n'importe quel individu

était une tâche ardue. À moins d'être célèbre, important ou soupçonné d'une infraction grave, la vie privée pouvait être relativement sûre sans devoir déployer beaucoup d'efforts pour s'en assurer.

L'avènement de la tenue électronique de dossiers a changé tout cela, éliminant les obstacles liés au temps, à la distance et au coût qui assuraient déjà notre vie privée. De nouvelles technologies de surveillance : les témoins et les dispositifs d'écoute sur le Web, les caméras vidéo, la surveillance du courrier électronique, les cartes intelligentes, les identificateurs biométriques, les dispositifs de repérage, les tests de dépistage de drogues, nous assaillent où que nous soyons. Des étrangers assis à leur ordinateur dressent des dossiers complets sur nous en quelques secondes. Nos activités et nos intérêts, nos achats et nos déplacements, nos opinions et nos habitudes sont consciencieusement consignés, analysés et classés pour quelque usage auquel le plus offrant veut les destiner.

Maintenant que la protection « par défaut » disparaît, il nous revient de prendre la barre.

Comme je l'ai mentionné ci-dessus, un des faits les plus intéressants que j'ai observé l'an dernier est que les plus grandes menaces à la vie privée viennent rarement des personnes qui veulent y porter atteinte.

IL FAUT VOIR
LA VIE PRIVÉE,
NON COMME
UN INTÉRÊT
INDIVIDUEL
ÉGOÏSTE QUI
DOIT CÉDER
LA PLACE
AUX BESOINS
SOCIAUX PLUS
IMPORTANTES,
MAIS BIEN
COMME UN
INTÉRÊT SOCIAL,
COMMUN ET
COLLECTIF,
CE QU'IL EST
DE FAIT.

Ces menaces viennent de personnes bien intentionnées qui affirment que la vie privée doit être sacrifiée à quelque bien supérieur – le service à la clientèle amélioré, la prévention de la criminalité, l'avancement de la science, la prestation plus efficace de programmes gouvernementaux, la sécurité.

Bien entendu, il arrive parfois que la vie privée cède le pas à d'autres intérêts sociaux.

Mais il nous faut nous demander, et demander à ces personnes bien intentionnées, quel genre de société nous desservirons, construirons et appuierons si la suppression de la vie privée est le prix que nous nous apprêtons à payer si volontiers.

Il faut voir la vie privée, non comme un intérêt individuel égoïste qui doit céder la place aux besoins sociaux plus importants, mais bien comme un intérêt social, commun et collectif, ce qu'il est de fait.

Voilà pourquoi c'est une importante période pour le Commissaire à la protection de la vie privée.

Il s'agit également d'une période importante pour une nouvelle loi sur la protection de la vie privée pour le secteur privé. Pendant près de 20 ans, nous avons une loi qui régissait la façon dont les gouvernements recueillaient et traitaient les renseignements personnels des Canadiens et Canadiennes. Mais c'est maintenant le secteur privé qui connaît une

explosion d'activités de collecte de renseignements et de constitution de dossiers personnels. Et c'est là où il faut de toute urgence exercer un contrôle sur les renseignements personnels.

Le Parlement a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* il y a près de deux ans, et celle-ci est entrée en vigueur le 1^{er} janvier 2001. La *Loi* constitue un important outil qui permettra aux Canadiens et Canadiennes d'exercer de nouveau un contrôle sur leurs renseignements personnels et de s'intéresser à protéger et à préserver leur vie privée.

La *Loi* vise les renseignements personnels recueillis, utilisés ou communiqués dans le cadre des activités commerciales. Elle repose sur un code modèle de protection des renseignements personnels, qui a été élaboré conjointement par les entreprises, le gouvernement et les groupes de consommateurs. Le code est fondé sur des principes largement reconnus liés à des pratiques équitables en matière de renseignements, y compris ceux établis par l'Organisation de la coopération et du développement économiques en 1980.

En bref, la *Loi* porte ce qui suit :

- Hormis certaines exceptions fort limitées, il est interdit aux organisations du secteur privé de recueillir, d'utiliser ou de communiquer vos renseignements personnels sans votre consentement.

- L'organisation peut recueillir, utiliser ou communiquer vos renseignements seulement pour les fins auxquelles vous avez consenti.
- Même avec votre consentement, l'organisation peut seulement recueillir les renseignements qu'une personne raisonnable estimerait acceptables dans les circonstances.
- Les personnes ont le droit d'accéder aux renseignements personnels qui sont détenus à leur sujet et de corriger toute inexactitude.
- Le Commissariat et moi-même exerçons une surveillance de façon à assurer le respect de la *Loi*. Des mesures de recours sont offertes aux personnes dont les droits ont été violés.

La *Loi* entre en vigueur en étapes successives. Elle s'applique depuis janvier 2001 aux renseignements personnels, à l'exception des renseignements sur la santé, des clients ou des employés d'entreprises de compétence fédérale, surtout les banques, les entreprises de télécommunications, de radiodiffusion et de transport interprovincial ou international, ainsi que celles dans les Territoires du Nord-Ouest, du Yukon et du Nunavut, où la *Loi* s'applique au secteur privé qui, aux termes de la Constitution, est réglementé par le fédéral.

La *Loi* vise également les renseignements personnels – de nouveau, autres que ceux sur la santé – lorsque ceux-ci sont communiqués à l'extérieur d'une province ou du pays pour contrepartie. Dans le jargon juridique, « communiqué pour contrepartie » signifie qu'on obtient quelque chose en échange des renseignements, par exemple, dans le cadre de ventes, de locations ou d'échanges. Les renseignements personnels eux-mêmes doivent faire l'objet d'un échange pour que la *Loi* soit applicable.

L'exclusion des renseignements personnels sur la santé était un compromis de dernière minute et n'est que temporaire.

Lorsque la *Loi* suivait le processus parlementaire, des représentants du secteur de la santé ont soulevé deux ensembles distincts et opposés de préoccupations. Certains voulaient une loi plus sévère, assortie de dispositions en matière de consentement plus contraignantes et des restrictions sur l'utilisation ultérieure des renseignements personnels sur la santé. D'autres étaient d'avis que la *Loi* restreindrait les activités opérationnelles dans le milieu de la santé et voulaient qu'elle soit plus permissive.

Pourtant, il n'y avait pas de problèmes ou d'obstacles fondamentaux à surmonter. Tout le monde reconnaissait que les renseignements personnels sur la santé devaient être protégés. À ce temps-là et depuis, personne n'a présenté d'indications claires et particulières pourquoi

LES
RENSEIGNEMENTS
PERSONNELS
SUR LA SANTÉ,
QUI PORTENT
SUR L'ÉTAT
DE NOTRE CORPS
ET DE NOTRE
ESPRIT, SONT,
COMME ON PEUT
LE SOUTENIR,
LES PLUS
PRIVÉS DE TOUS.

la *Loi*, telle qu'elle était libellée, ne pouvait être efficace. En effet, comme l'a indiqué le ministre de la Santé d'alors, David Dodge, lors de sa comparution devant un comité du Sénat :

Cela fait environ six mois que je demande des renseignements précis sur ce qui pourrait déraiper si le projet de loi était adopté, tel que prévu dans un an. J'ai exercé des pressions afin de déterminer les choses qui pourraient ne pas fonctionner et ce que nous ne pourrions faire. Franchement, j'ai été surpris que malgré les critiques générales et l'incertitude, je n'ai toujours pas eu d'exemples de choses qui pourraient mal tourner. Parce que nous sommes en territoire inconnu, il en découle des doutes et de l'incertitude. Toutefois, on ne m'a toujours pas fourni d'exemples de choses qui pourraient de fait mal tourner.

[traduction libre]

On a éventuellement convenu d'exclure les renseignements sur la santé de la *Loi* durant une période d'un an après son entrée en vigueur, de façon à accorder au secteur de la santé suffisamment de temps pour s'adapter à la nouvelle *Loi*.

Récemment, des efforts de lobbying déterminés ont été déployés par divers intérêts puissants du secteur de la santé pour continuer à priver les Canadiens et Canadiennes de la protection des renseignements personnels sur la santé,

dont l'entrée en vigueur était prévue pour le 1^{er} janvier. Certains ont exercé des pressions pour qu'on prolonge l'exclusion des renseignements personnels sur la santé. D'autres encore aimeraient que la *Loi* soit modifiée de diverses façons, notamment en adoptant un régime réglementaire distinct qui passerait outre aux dispositions de la *Loi* et éliminerait le rôle de surveillance joué par le Commissaire à la protection de la vie privée.

Mais deux choses sont demeurées constantes depuis l'an dernier. Tout d'abord, on n'est toujours pas parvenu à recueillir un large consensus, car certains sont toujours favorables à une loi plus sévère, tandis que d'autres veulent l'affaiblir. En second lieu, personne n'est encore parvenu à démontrer de façon précise et persuasive ce qui cloche avec le libellé de la *Loi*.

À mon avis, tout délai ou affaiblissement de la protection des renseignements personnels sur la santé, à laquelle s'attendent les Canadiens et Canadiennes comme leur a promis le Parlement, représenterait un terrible coup porté aux droits à la vie privée.

Les renseignements personnels sur la santé, qui portent sur l'état de notre corps et de notre esprit, sont, comme on peut le soutenir, les plus privés de tous. Toute communication induite peut comporter des conséquences dévastatrices. En effet, la crainte de ne plus pouvoir exercer de contrôle sur leurs

renseignements personnels sur la santé peut empêcher des personnes de demander des soins médicaux, ce qui comporterait des résultats préjudiciables non seulement pour ces personnes mais également pour la société dans son ensemble. C'est pourquoi, une loi sur la protection de la vie privée qui ne garantit pas pleinement la protection des renseignements personnels sur la santé n'est pas acceptable. La prorogation d'un an accordée à cet égard est plus que suffisante.

Une inquiétude encore plus grande tient au fait que tout délai ou affaiblissement de la protection des renseignements personnels sur la santé réduise l'efficacité de la LPRPDÉ dans l'ensemble. Les intervenants du milieu de la santé peuvent soutenir que leur secteur est visé par des questions spéciales et distinctes en matière de vie privée. Mais les intervenants du milieu bancaire, des transports et des télécommunications, somme toute de n'importe quel secteur de l'économie, pourraient facilement soutenir le même argument.

C'est pourquoi, la *Loi* a été rédigée sur la base de principes et de règles relativement larges, en accordant une marge de manœuvre et une interprétation fort amples relativement à son application. Si des exceptions spéciales devaient être accordées à un secteur, comme celui de la santé, tous les autres secteurs pourraient demander un traitement de faveur,

et toute la structure sur laquelle repose la *Loi sur la protection des renseignements personnels* s'écroulerait.

J'ai été très heureux d'apprendre que le ministre de la Santé, l'honorable Allan Rock, abondait dans mon sens dans une lettre du 24 septembre qu'il m'a envoyée :

Je n'appuie pas la création d'un organisme de réglementation distinct qui se chargerait des renseignements personnels sur la santé aux termes de la LPRPDÉ. La *Loi*, qui a été adoptée par le Parlement il y a un peu plus d'un an, énonce clairement que la surveillance, les mesures de réparation et les responsabilités en matière de vérification reviennent au Commissaire à la protection de la vie privée. Le sous-ministre a également clairement indiqué aux intervenants du secteur de la santé que nous n'envisageons pas de modifications à la LPRPDÉ en vue de créer un organisme distinct pour le secteur de la santé, et que nous n'appuyons pas de prorogation de l'application de la LPRPDÉ au secteur de la santé. [traduction libre]

Je suis reconnaissant au ministre de la Santé d'avoir reconnu, pour le compte de son ministère, l'importance vitale de l'entrée en vigueur de la protection des renseignements personnels sur la santé, telle que prévue le 1^{er} janvier 2002.

IL EST
 IMPORTANT
 DE SOULIGNER
 QU'IL RESTE
 DEUX ANS AU
 SECTEUR DE
 LA SANTÉ POUR
 SE PRÉPARER
 À L'ENTRÉE EN
 VIGUEUR DE
 LA *LOI* DANS
 LES DOMAINES
 QUI LE
 PRÉOCCUPENT
 LE PLUS.

Au moment de rédiger le présent rapport, il semblait en effet que la *Loi* sera appliquée telle qu'elle a été libellée. Le 1^{er} janvier 2002, les renseignements personnels sur la santé détenus par les entreprises fédérales sur leurs clients ou employés seront protégés.

La vente ou l'échange de renseignements personnels sur la santé à l'extérieur d'une province ou du pays est également visé par la *Loi*. La communication de renseignements personnels sur la santé au-delà des territoires pour contrepartie (dans la mesure où la contrepartie vise les renseignements) sera couverte. En outre, toutes les entreprises et les organisations au Yukon, dans les Territoires du Nord-Ouest et au Nunavut qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales devront également assurer la protection des renseignements personnels sur la santé.

Il est important de souligner qu'il reste deux ans au secteur de la santé pour se préparer à l'entrée en vigueur de la *Loi* dans les domaines qui le préoccupent le plus. Ainsi, la *Loi* s'appliquera seulement directement aux services commerciaux touchant la santé, tels que ceux fournis par les cabinets de médecin, les cliniques privées, les laboratoires et les pharmacies, que le 1^{er} janvier 2004. À cette date, la *Loi* s'appliquera à toutes les activités commerciales du secteur privé dans les provinces, sauf lorsqu'une province a adopté une loi essentiellement similaire.

J'aimerais aborder une question particulière à ce point-ci.

Je sais que les intervenants du milieu de la santé sont préoccupés à juste titre au sujet de l'incidence possible de la *Loi* sur la recherche sur la santé, car elle vise des renseignements personnels sur la santé et des considérations pécuniaires qui peuvent être en cause. J'aimerais préciser que la recherche sur la santé en bonne et due forme, qui est entreprise avec sensibilité relativement aux droits à la vie privée des Canadiens et Canadiennes, n'a rien à craindre de la *Loi* ou du Commissariat.

Ma position sur cette importante question est la suivante :

Les renseignements personnels sur la santé représentent sans doute les renseignements personnels de nature la plus hautement délicate touchant la vie privée et, en règle générale, les individus doivent pouvoir exercer un droit de regard sur les personnes qui peuvent recueillir, utiliser ou communiquer ces renseignements ainsi que les fins pour lesquelles elles le font. Parallèlement, toutefois, notre société s'intéresse à juste titre à la poursuite et à l'accroissement de la recherche sur la santé, qui promet d'importants bénéfices à tous les individus.

La clause sur l'objet de la *Loi* précise que les règles visent à équilibrer le « droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir,

d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ».

Concernant la recherche sur la santé, il me semble qu'il soit clair qu'un juste équilibre permet de protéger les intérêts authentiques des individus en matière de vie privée, tout en permettant la conduite de recherches légitimes sur la santé, qui utilisent les renseignements sans comporter d'incidence possible sur les individus auxquels ils se rapportent. Je ne crois pas que l'objet de la *Loi* était d'empêcher ou d'entraver de quelque façon que ce soit la recherche, et mes homologues provinciaux et territoriaux avec qui j'ai discuté de cette question cet été partageaient mon avis.

Par conséquent, j'ai l'intention d'interpréter largement l'objet de l'alinéa 7(2)c) de la *Loi* qui autorise une organisation à utiliser les renseignements personnels à l'insu de l'intéressé et sans son consentement dans la mesure où « l'utilisation est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites, ces fins ne peuvent être réalisées sans que le renseignement soit utilisé, celui-ci est utilisé d'une manière qui en assure le caractère confidentiel, le consentement est pratiquement impossible à obtenir et l'organisation informe le Commissaire de l'utilisation avant de la faire ». L'alinéa 7(3)f) comprend une disposition parallèle visant la communication des renseignements personnels à l'insu de l'intéressé ou sans son consentement.

Je suis d'avis que la recherche sur la santé authentique entreprise par des organisations dûment agréées et qui est assortie de mesures de sauvegarde indiquées représente de fait une étude ou une recherche statistique ou savante, et ce, que des intérêts pécuniaires soient engagés ou non. Du simple fait que la recherche sur une condition médicale donnée puisse bénéficier d'une aide au financement d'une source extérieure, qui espère tirer des gains financiers de la découverte d'un nouveau médicament efficace, par exemple, ne modifie nullement à mon avis sa légitimité en tant que recherche sur la santé d'un point de vue des droits à la vie privée.

Concernant l'impossibilité d'obtenir un consentement pour une telle recherche, je reconnais le bien-fondé de la position du milieu de la recherche sur la santé, à savoir que des facteurs de coûts ou la difficulté d'obtenir le consentement auprès de 100 % de la population cible font qu'il est impraticable d'obtenir le consentement individuel pour bon nombre d'études sur la santé.

La *Loi* exige que les renseignements en question soient utilisés de façon à en assurer la confidentialité. Je crois que cette exigence est d'importance primordiale.

J'adopterai en conséquence la position selon laquelle les renseignements personnels sur la santé peuvent être communiqués et utilisés sans consentement aux fins de la recherche sur la santé décrite ci-dessus, mais seulement dans

“ BREF, NOUS
JUIRONS
BIENTÔT D'UNE
PROTECTION
HOMOGÈNE DE
LA VIE PRIVÉE
AU CANADA.

la mesure où ceux-ci sont strictement confinés par le projet de recherche et que les individus qu'il concerne ne subissent aucun préjudice.

Sans restreindre la portée générale de ce qui précède, je considère comme une exigence absolue que la communication et l'utilisation des renseignements personnels sur la santé sans le consentement des personnes visées, aux fins de la recherche sur la santé, ne peuvent de quelque façon que ce soit parvenir à l'employeur, à l'assureur, aux parents ou aux connaissances de l'individu, ni aux autorités gouvernementales ou aux forces de l'ordre, aux mercaticiens ou à tout autre tiers. Il est en outre interdit à quiconque, autre que le médecin de l'individu ou tout autre fournisseur principal des soins de santé, le cas échéant, de communiquer avec l'individu en raison de ces renseignements.

Le Commissariat et moi-même assurerons une surveillance vigilante de cette exigence, et tout manquement sera considéré, de plein droit, comme une violation extrêmement grave de la *Loi*.

Je suis convaincu que cette démarche satisfera pleinement l'esprit de la *Loi*, permettra de protéger efficacement les droits à la vie privée des Canadiens et Canadiennes, et toute recherche légitime sur la santé pourra être menée sans entrave.

La dernière étape de la mise en œuvre de la *Loi* débutera en janvier 2004. À ce temps-là, celle-ci visera toutes les activités commerciales au Canada, sous réserve d'une importance exemption : lorsqu'une province a adopté une loi sur la vie privée essentiellement similaire, le gouvernement fédéral peut exempter les organisations et les activités dans la province de l'application de la loi fédérale, et la loi provinciale aura préséance.

Les entreprises réglementées par le fédéral dans ces provinces continueront d'être régies par la *Loi* fédérale ainsi que les échanges de renseignements personnels entre les organisations à l'extérieur d'une province ou à l'étranger dans le cadre de leurs activités commerciales.

Bref, nous jouirons bientôt d'une protection homogène de la vie privée au Canada. Tout le secteur privé devra se conformer à la loi fédérale ou à une loi provinciale essentiellement similaire.

Une des remarques au sujet de la nouvelle loi pour le secteur privé que j'ai faite fréquemment l'an dernier, surtout devant des auditoires de gens d'affaires, est que la *Loi* ne démarque pas le Canada du reste du monde. Des lois semblables ont été adoptées dans la majorité des pays les plus évolués d'un point de vue économique, à l'exception des États-Unis. Même là, le débat porte moins sur les principes que sur la meilleure façon de les observer.

J'AI DÉCIDÉ DÈS LE DÉPART DE METTRE UN ACCENT SPÉCIAL
SUR LA COMMUNICATION.

Une des raisons pour lesquelles ce genre de loi est adoptée est que lorsqu'un pays en a promulgué une, il ne peut assurer l'entière protection des renseignements de ses citoyens que si les pays avec lesquels il fait des échanges offrent une protection semblable. Afin de favoriser une meilleure compréhension de notre façon de protéger la vie privée au Canada, j'ai prononcé des discours et participé à des conférences à Washington, à l'Université Harvard, ainsi qu'à Bruxelles, à Cambridge et à Londres, et je me suis entretenu avec des commissaires à la protection de la vie privée et aux données nominatives partout sur la planète.

Lorsque j'ai été nommé Commissaire à la protection de la vie privée, j'ai examiné la situation qui existait, c'est-à-dire les multiples menaces à la vie privée qui découlait d'objectifs sociaux raisonnables, les attentes de plus en plus limitées face à la vie privée, une nouvelle loi complexe, et un public qui, dans une certaine mesure, semblait tellement habitué à voir sa vie privée s'amenuiser qu'il courait le risque de perdre de vue la signification et l'importance de celle-ci.

Compte tenu de tout cela, j'ai décidé dès le départ de mettre un accent spécial sur la communication.

Une des premières mesures que j'ai prises en tant que Commissaire à la protection de la vie privée a été de créer la Direction des communications et des analyses stratégiques au sein

du Commissariat, qui serait chargée de mener des recherches sur les questions touchant la vie privée et de joindre le public afin de le renseigner et d'obtenir ses avis. Et j'ai personnellement saisi toutes les occasions qui m'étaient offertes de transmettre mon message, me rendant aux quatre coins du pays, prenant la parole lors de conférences et de réunions, et accordant des entrevues aux médias.

J'ai également veillé à ce que le public ait accès à des renseignements exacts et courants sur notre site Web. Les discours, par exemple, que je prononce y sont affichés en version publiée dès que je les ai livrés. Nous avons fait paraître des trousseaux d'information sur des sujets variés, y compris le vol d'identité, le recensement et, bien entendu, comment accéder aux renseignements personnels et faire valoir ses droits aux termes des lois canadiennes sur la vie privée. Nous avons également publié des guides complets à l'intention des individus et des entreprises sur la nouvelle loi et son incidence sur ces derniers.

J'ai fait tout cela parce qu'il est très important que les Canadiens et Canadiennes soient bien renseignés sur leurs droits et qu'ils comprennent les implications de la perte de leur vie privée. Et en bout de ligne, je dois avouer que je compte sur l'appui du public dans mon rôle d'ombudsman, qui est mon principal recours afin d'assurer la protection des droits

“ L’AN DERNIER, LES ACTIVITÉS DE SURVEILLANCE SE SONT ACCRUES, À LA FOIS PAR LES GOUVERNEMENTS ET LE SECTEUR PRIVÉ, CE QUI A PLACÉ CETTE QUESTION À L’AVANT-PLAN DE NOS PRÉOCCUPATIONS.

des Canadiens et Canadiennes aux termes de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Je ne suis pas investi de pouvoirs officiels en vue de contraindre les institutions fédérales et les entreprises du secteur privé à respecter la vie privée des personnes, ou à faire réparation à ces dernières de tout manquement. Je peux faire appel aux tribunaux dans certaines situations, bien entendu, mais ce n’est jamais une solution optimale. Je fais surtout appel au pouvoir qu’exerce l’opinion publique. Peu de personnes, que ce soit dans les gouvernements ou les entreprises, veulent mécontenter le public. D’ailleurs, plus le public est mieux informé, plus son opinion sera respectée.

J’aimerais maintenant revenir, comme j’ai dit que je le ferais, à certaines questions précises touchant la vie privée qui m’ont interpellé cette année.

La surveillance – la surveillance visuelle factuelle – a longtemps été une principale préoccupation des défenseurs des droits à la vie privée. L’an dernier, les activités de surveillance se sont accrues, à la fois par les gouvernements et le secteur privé, ce qui a placé cette question à l’avant-plan de nos préoccupations.

La vie privée signifie être en mesure de mener des activités licites sans que chacun des gestes posés soient surveillés de près. Bien que nous devions nous soucier des menaces à la vie privée subtiles que présentent la collecte et la gestion modernes des renseignements, il est impératif de ne pas perdre de vue la violation flagrante de la vie privée que représente la surveillance.

La surveillance vidéo est omniprésente, dans les espaces publics et privés. Nous sommes devenus tellement conditionnés à être surveillés et enregistrés lorsque nous sommes dans une banque ou un dépanneur, lorsque nous nous déplaçons dans un aéroport ou que nous franchissons une intersection. Et maintenant, ce qui est plus alarmant, nous voyons une tendance accrue de la surveillance quand nous marchons dans les rues de nos villes.

Les personnes qui se trouvent dans un espace public peuvent raisonnablement s’attendre à être observées par d’autres. C’est une chose de s’exposer aux regards fortuits d’autrui ou même de susciter un intérêt auprès de nos concitoyens, mais s’en est une autre d’être observés de façon systématique et ininterrompue, sans motif valable, par des agents de l’État.

Nous n'en sommes toutefois pas au même point que le Royaume-Uni, où un réseau croissant de surveillance vidéo, comptant deux millions de caméras vidéo selon un rapport récent, surveille les rues, les stationnements, les quartiers et les centres commerciaux.

Nous n'avons pas non plus emboîté le pas aux États-Unis, où on pratique déjà la surveillance vidéo aléatoire de rassemblements publics et où on utilise des bases de données biométriques, ce qui constitue l'équivalent électronique d'un alignement de confrontation de la police, où chacun doit participer, qu'il soit soupçonné ou non de méfaits.

Nous avons vu des systèmes de surveillance vidéo installés dans des rues publiques à Kelowna (C.-B.) – ce qui a fait l'objet d'une plainte au Commissariat – et des systèmes semblables sont prévus dans diverses autres villes canadiennes.

En outre, la technologie biométrique de reconnaissance de visage, dans les casinos en Ontario et à l'Aéroport international Pearson de Toronto, a également fait les manchettes cette année. (Dans cette dernière affaire, les reportages se sont avérés erronés; mon enquête a révélé que la GRC fait un usage raisonnable de la technologie biométrique. Le lecteur peut se reporter au compte rendu de cette affaire dans la première partie du présent rapport.)

La justification de la surveillance est toujours la même : elle accroît la sécurité et dissuade le crime. Ces raisons ne peuvent être écartées du revers de la main. Qu'il s'agisse de voler une banque ou de brûler un feu rouge, les défenseurs des droits à la vie privée ne tolèrent pas que des personnes invoquent le respect de la vie privée pour excuser les manquements délibérés aux règles et aux lois de la société.

Mais, comme quelqu'un l'a déjà dit, le seul endroit où les agents policiers ont la tâche facile, c'est dans un État policier. Nous ne pouvons laisser les préoccupations légitimes au sujet de la sécurité éclipser les préoccupations légitimes au sujet de la vie privée. Si nous mettons tout le monde dans le même bateau, si tout le monde devient un suspect dont chaque agissement doit être surveillé et peut-être enregistré, analysé et classé, juste au cas, il se peut que nous ayons fait tout ce que nous pouvons pour empêcher le crime et exercer un contrôle sur lui. Mais nous l'aurons fait au détriment du respect d'un droit de la personne fondamentale.

Si l'État n'a pas raison de surveiller les citoyens respectueux des lois, le secteur privé l'a encore moins. Pourtant cette année, une entreprise de sécurité privée à Yellowknife a décidé de faire de la surveillance publique son affaire, et a braqué ses caméras vidéo sur une rue au centre-ville. Cela a suffi pour qu'une plainte

CE QU'IL FAUT SOULIGNER INSTAMMENT DANS CETTE AFFAIRE, C'EST QU'IL N'Y A ABSOLUMENT AUCUNE PREUVE QUE LA SURVEILLANCE VIDÉO RÉDUIT DE FAIT LA CRIMINALITÉ, AU LIEU DE TOUT SIMPLEMENT LA DÉLOGER VERS D'AUTRES ENDROITS OÙ IL N'Y A PAS DE CAMÉRAS.

soit déposée aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui s'applique à toutes les activités du secteur privé dans les Territoires. J'ai indiqué mes conclusions à ce sujet dans la deuxième partie du présent rapport, et je me contenterai de dire que cette pratique contrevenait à la *Loi*. Je crois que nous pouvons tous être satisfaits d'apprendre que cette entreprise n'a pas joui de l'appui des représentants municipaux, des forces policières ou du public, et qu'elle a accepté volontiers de mettre fin à ses activités de surveillance lorsque le public s'y est opposé.

Ce qui est encore plus perturbant, c'est la situation à Kelowna, en Colombie-Britannique. La GRC, à titre de force policière municipale, a installé une caméra vidéo pour surveiller de façon continue et enregistrer tous les passants dans une rue publique. En enquêtant sur une plainte qu'avait déposée au Commissariat le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, j'ai conclu que cette activité de collecte de renseignements personnels constituait une contravention claire à la *Loi sur la protection des renseignements personnels*.

Pourtant, la GRC poursuit sa surveillance vidéo jour et nuit, mais sans effectuer d'enregistrement continu des déplacements. Ce faisant, la GRC est techniquement conforme à la *Loi sur la protection des renseignements personnels*, où il est défini que les renseignements personnels sont des renseignements sur un individu

identifiable qui sont « consignés sous une forme ou autre ».

Comme je l'ai montré clairement dans ma conclusion, je considère cette forme de surveillance vidéo des endroits publics comme une violation extrêmement grave des droits à la vie privée, même en l'absence d'un enregistrement. C'est la présence même des caméras vidéo, qu'elles enregistrent ou non à un moment donné, qui suscite le sentiment d'être observé et qui sape la vie privée. De plus, si nous permettons la prolifération des caméras vidéo, il est presque certain que l'implantation progressive de cette fonction entraînera inexorablement l'association des caméras et de la technologie biométrique. Ainsi, il se peut qu'il soit éventuellement possible d'identifier toute personne qui se trouve dans un endroit public sous surveillance continue, ou de surveiller les allées et venues et les activités d'un individu donné alors qu'il se déplace d'un endroit à l'autre.

Ce qu'il faut souligner instamment dans cette affaire, c'est qu'il n'y a absolument aucune preuve que la surveillance vidéo réduit de fait la criminalité, au lieu de tout simplement la déloger vers d'autres endroits où il n'y a pas de caméras. De fait, un porte-parole du détachement de la GRC à Kelowna, le caporal Reg Burgess, a déclaré le 19 juin 2001 au *Vancouver Sun*, que ces caméras « peuvent dans certaines circonstances prévenir le crime, mais qu'elles réussissent surtout à le déplacer ». [traduction libre]

Le journaliste de cet article du *Vancouver Sun* a poursuivi en disant : « M. Burgess a ajouté qu'en déplaçant le crime hors du centre-ville de Kelowna vers les quartiers résidentiels, la police serait alertée d'activités criminelles plus rapidement par les résidents. »
[traduction libre]

Parce que mon mandat prévoit que je surveille l'application des lois sur la vie privée plutôt que l'application des lois générales, il n'est probablement pas de mon ressort de commenter la politique sur l'utilisation des caméras vidéo de la GRC en vue de déplacer la criminalité des centres-villes vers les quartiers résidentiels.

Toutefois, j'ai récemment rencontré le Commissaire de la GRC, Giuliano Zaccardelli, et j'ai tâché tant bien que mal de le convaincre de respecter les droits à la vie privée en ordonnant le retrait des caméras de surveillance à Kelowna. Dans une lettre datée du 27 novembre 2001, M. Zaccardelli m'a répondu :

Je suis satisfait que dans le cas de Kelowna, la GRC exerce son devoir de protéger la collectivité en s'appuyant sur des préoccupations en matière de sécurité publique bien formulées. L'utilisation des caméras représentera un atout valable pour la collectivité et permettra de mettre fin aux activités criminelles et d'accroître la sécurité à cet endroit. [traduction libre]

J'ai alors demandé au Commissaire Zaccardelli de me fournir les données sur lesquelles il fonde ses conclusions, à savoir que la surveillance vidéo appuie effectivement la GRC dans son devoir de protéger la collectivité, et surtout la preuve que les caméras en opération depuis février dernier parviennent de fait à « mettre fin aux activités criminelles » et à faire de Kelowna un endroit plus sûr où vivre. Plus particulièrement, j'ai demandé au Commissaire Zaccardelli de me faire parvenir des statistiques sur le nombre d'arrestations qui découlent de l'utilisation de la caméra depuis février dernier ainsi que des statistiques comparant le taux de criminalité global à Kelowna durant les mois où la caméra était en opération avec le taux de criminalité pour la même période l'an dernier. Il ne m'a toujours pas fait parvenir ces renseignements.

Je trouve cette situation fort déplorable. On pourrait s'attendre que le Commissaire de la GRC, qui choisit de ne pas tenir compte d'une recommandation vigoureuse d'un haut fonctionnaire du Parlement dans une affaire aussi importante, fonde sa décision sur une preuve la plus contraignante qui soit, au lieu de l'appuyer sur des conjectures non corroborées ou des idées chimériques.

Ce qui est plus important, c'est qu'on pourrait s'attendre d'un agent de police du plus haut rang au Canada, c.-à-d. le dirigeant de la force policière nationale, qu'il veuille que celle-ci donne l'exemple en établissant les normes les

“ J’AI
RESPECTUEUSEMENT
DEMANDÉ LE
CONCOURS DES
DÉPUTÉS ET
DES SÉNATEURS
AFIN DE
PERSUADER
LE COMMISSAIRE
ZACCARDELLI
POUR QU’IL
RÉVISE SA
POSITION
RELATIVEMENT À
CETTE AFFAIRE. ”

plus rigoureuses qui soient concernant le respect des droits à la vie privée. J’ai bon espoir que le Commissaire Zaccardelli conviendra éventuellement du bien-fondé de cette avis. S’il persiste toutefois dans sa position actuelle sur la surveillance vidéo, il donnera malheureusement un tout autre exemple, que suivront les forces policières partout au pays.

Le niveau et la qualité de la vie privée au pays risquent d’être assésés, un coup démoralisant et irréparable si nous permettons d’être surveillés et observés constamment de manière constante and ininterrompue par des caméras vidéo en prolifération qui sont sous le contrôle de la police ou d’autres agents de l’État.

C’est pourquoi, j’ai respectueusement demandé le concours des députés et des sénateurs afin de persuader le Commissaire Zaccardelli pour qu’il révisé sa position relativement à cette affaire. Cette question est pour moi de la plus grande importance.

La surveillance vidéo est le moyen le plus évident par lequel nous sommes surveillés et observés en public. Mais il y en a d’autres. La technologie de repérage qui est installée dans les téléphones cellulaires permet de situer l’emplacement d’un utilisateur dans un rayon de 50 mètres. La technologie de positionne-

ment géographique peut servir à localiser les véhicules. Les systèmes de paiement électronique utilisés sur les routes et les ponts à péage peuvent également être utilisés pour suivre le déplacement des véhicules.

Nous avons bien dépassé ce que « sortir en public » signifiait autrefois. Lorsque nous sommes en public, nous sommes *réellement* en public; il semble qu’il n’y ait rien qui soit privé.

Et ce qui accuse le problème, à mesure que la distinction entre ce qui est public et privé s’estompe, l’assaut porté contre la vie privée en public gagne les domaines que nous considérons déjà comme indiscutablement privés. Un nombre croissant de technologies d’amplification sensorielle, les capteurs chimiques et à ondes acoustiques, les dispositifs à imagerie thermique, les jumelles à infrarouge, les appareils portatifs à rayons X, permettent « d’écouler » dans les endroits publics ce qui se passe dans les endroits privés et fermés. La célèbre affaire *Kyllo* aux États-Unis, où une opération clandestine de culture de marijuana a été repérée au moyen d’un dispositif à imagerie thermique qui a capté la transmission thermique à l’extérieur de la maison, montre à quel point la distinction entre ce qui est public et privé est floue.

De nouveau, les défenseurs des droits à la vie privée ne plaident pas la cause de la criminalité. Ils reconnaissent les bonnes intentions de ceux qui veulent recourir à la surveillance pour accroître la sécurité. Mais notre société peut atteindre ses objectifs légitimes en matière de sécurité et de prévention de la criminalité sans toutefois se défaire des droits à la vie privée et des libertés civiles fondamentales qui en découlent. Ces technologies intrusives dans la vie privée doivent être confinées à des situations limitées et particulières, où la menace à la sécurité publique est matérielle, importante et imminente, et elles doivent être visées par une autorisation judiciaire préalable, autrement dit, être assorties de mandats.

Même l'accroissement extraordinaire de l'utilisation généralisée de la surveillance exercée sur notre personne publique par les agents de l'État, n'est rien comparativement à l'explosion de la surveillance des employés à la fois en milieu de travail et hors de celui-ci. Il s'agit d'une question qui m'inquiète de plus en plus.

Comme je l'ai mentionné lors d'une conférence à Toronto en avril dernier, la vie privée en milieu de travail est une question qui a pris de plus en plus d'importance, car la protection implicite de la vie privée n'est

plus suffisante. En outre, les droits à la vie privée en milieu de travail ne sont pas bien définis, car jusqu'à présent, il n'était pas nécessaire qu'ils le soient.

Les gestionnaires ont toujours voulu assurer le rendement et prévenir la redevabilité. Même avant que Henry Ford et Frederick Taylor n'aient mis en place la chaîne de montage et la « gestion scientifique », les gestionnaires surveillaient, mesuraient et exerçaient un contrôle sur les travailleurs.

Mais pendant longtemps, la technologie imposait une limite bénigne à tout cela. Les travailleurs pouvaient maintenir leur vie privée lorsqu'ils étaient au travail, au même titre qu'ils assuraient la confidentialité du contenu de leurs tiroirs de bureau, casiers et de leurs effets personnels, du simple fait que la surveillance et l'enregistrement pouvaient aisément être surchargés de renseignements.

Cette limite bénigne a commencé à disparaître lorsque l'usage des ordinateurs s'est répandu. L'illusion d'une sécurité et d'un contrôle parfaits est pratiquement réalisable en milieu de travail, en raison de la technologie qui permet aux gestionnaires de surveiller tous les déplacements et d'analyser tout ce qui est enregistré.

LES EMPLOYÉS
NE RENONCENT
PAS À
LEUR DROIT
FONDAMENTAL
À LA VIE
PRIVÉE
LORSQU'ILS
SIGNENT UN
CONTRAT DE
TRAVAIL.

La notion que les employés ont des droits à la vie privée en milieu de travail est inacceptable pour certains, parce que ceux-ci sont à l'emploi et dans les locaux de l'employeur, utilisant son matériel. Je ne suis pas d'accord. Les employés ne renoncent pas à leur droit fondamental à la vie privée lorsqu'ils signent un contrat de travail. Et cela peut en surprendre certains qu'un nombre considérable de juges et d'arbitres partagent mon avis.

Néanmoins, nous avons été témoin d'un extraordinaire accroissement de la surveillance en milieu de travail. Cela est surtout apparent aux États-Unis, où il n'y a pas de loi en vigueur pour assurer la protection de la vie privée des employés. En janvier 2001, l'American Management Association a sondé 1 627 moyennes et grandes entreprises et a révélé que plus de 75 % d'entre elles font un enregistrement vidéo de leurs employés ou surveillent leur courrier électronique, leur utilisation d'Internet, leurs conversations téléphoniques ou leurs fichiers informatiques. Cela représente une augmentation de près de 10 % comparativement aux résultats d'un sondage semblable mené l'an dernier.

Il n'y a pas d'études comparables de l'ampleur de la surveillance des employés au Canada, mais on croit que la situation au pays reflète

celle aux États-Unis. Il se peut que cette hypothèse soit erronée, en partie parce qu'on ne comprend pas bien les différences qui existent entre les lois canadiennes et américaines.

Il arrive fréquemment qu'on ne soit pas au fait des particularités des lois au Canada. À titre d'exemple, les employeurs invoquent souvent leur responsabilité potentielle à l'égard du harcèlement en milieu de travail pour justifier une surveillance, surtout d'Internet et du courrier électronique. Cela reflète la doctrine juridique américaine, et non celle en vigueur au Canada. Au pays, la législation antidiscrimination reconnaît seulement une responsabilité à l'employeur lorsque celui-ci n'a pas pris de mesures raisonnables pour prévenir le harcèlement. Mais cela ne veut pas dire pour autant qu'il faut employer la surveillance électronique de façon généralisée en milieu de travail. Il faut plutôt adopter une politique antiharcèlement fondée, assurer la formation des employés, mettre en place des procédures antiharcèlement convenables (comme l'embauche d'un coordonnateur des initiatives antiharcèlement et un processus de plaintes confidentiel), et réagir rapidement et efficacement en l'occurrence de harcèlement ou lorsqu'on a de bonnes raisons de croire qu'il se produit.

LA SURVEILLANCE ÉLECTRONIQUE NE DOIT JAMAIS SE SUBSTITUER
AUX PRATIQUES DE GESTION ET DE SUPERVISION SAINES.

Une autre excuse qu'on avance parfois concernant la surveillance électronique généralisée est la « possibilité » de l'utilisation d'Internet qui représente une perte de temps et le mésusage du matériel de l'employeur. Je ne crois pas qu'on doive surveiller les employés pour prévenir des pertes de temps potentielles, pas plus que nous devons surveiller les citoyens respectueux des lois pour éviter la possibilité que l'un d'eux commette un crime. Les soupçons raisonnables de fautes doivent être la seule justification de la surveillance en milieu de travail. La surveillance électronique ne doit jamais se substituer aux pratiques de gestion et de supervision saines. Si la seule façon qu'a un employeur pour savoir si les employés travaillent, c'est de les surveiller avec des moyens électroniques, alors il y a quelque chose qui cloche avec les pratiques de gestion qu'il a adoptées.

La Loi sur la protection des renseignements personnels et les documents électroniques limite la collecte, l'utilisation et la communication de renseignements aux seules « fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Il s'agit d'une importante restriction de la surveillance en milieu de travail. Parce que la *Loi*, ou une loi provinciale similaire, aura bientôt force

exécutoire pour les employeurs partout au pays, ceux-ci auraient intérêt à en prendre connaissance.

J'ai mentionné ci-dessus les implications sur la vie privée qui découlent des pressions exercées pour assurer la transparence au sein des gouvernements et l'accès aux renseignements qu'ils détiennent. Cette question est arrivée au point critique cette année car diverses parties ont tenté d'avoir accès à l'emploi du temps du premier ministre, et ils étaient appuyés dans leur tentative par le Commissaire à l'information.

Que les valeurs de transparence et d'accès à l'information ont pu être déformées à ce point et constituer une attaque à la vie privée – les emplois du temps sont de par leur nature même privés – a été une bien pénible découverte pour moi. Je n'ai jamais cru que je m'opposerais à une demande d'accès à l'information. En tant qu'ancien journaliste, je suis sensibilisé au plus haut point à l'importance de la transparence au sein des gouvernements. Et en tant que citoyen activement engagé, j'ai vu comment il est possible d'accroître la responsabilité en rendant facilement accessible l'information.

Mais cette bonne intention ne peut ni tout invalider ni justifier la violation du droit à la vie privée individuelle. De nouveau, il faut défendre la vie privée dans toute son importance sociétale, en tant que droit fondamental, de façon que celle-ci ne soit pas perçue comme quelque chose à échanger chaque fois qu'on y voit un obstacle à un objectif valable.

Heureusement, je ne suis pas le seul à m'inquiéter à ce sujet. Les tribunaux ont été très clairs : la transparence du gouvernement n'empêche pas la protection des droits humains fondamentaux. L'accès est un droit administratif qui peut rehausser la démocratie. Et la vie privée est un droit humain fondamental qui est de l'essence même de la démocratie.

Une autre importante question est l'initiative Gouvernement en direct. La transition à une interface électronique homogène entre les citoyens et les divers paliers de gouvernement peut s'avérer bénéfique, améliorant la prestation des programmes ainsi que l'efficacité et l'accessibilité des gouvernements. Tous les Canadiens et Canadiennes ont une histoire à raconter au sujet de la confusion concernant le ministère ou le palier d'administration chargé d'un service donné auquel faire appel. Et bon nombre de Canadiens et Canadiennes connaissent des histoires, qu'elles soient vraies ou anecdotiques, au sujet des difficultés éprouvées lorsqu'on tente d'obtenir des renseignements du gouvernement.

Mais les distinctions entre les organismes et les programmes, au sein du gouvernement ou dans l'ensemble des paliers de gouvernement, présentent des obstacles à la collecte de renseignements personnels. Le gouvernement en tant qu'organisme unique et centralisé rend possible la fusion des bases de données, qui renferment des renseignements sur les interactions des particuliers avec le gouvernement. Ces renseignements ont été recueillis à des fins particulières. Lorsque les renseignements sont conservés dans des bases de données distinctes pour des usages particuliers, ils sont compartimentés.

Lorsque les bases de données sont fusionnées, une personne qui a besoin d'un seul élément d'information peut avoir accès à bon nombre de renseignements. Et tout renseignement peut être combiné seulement à d'autres et révéler de nouveaux renseignements, rendant possible l'établissement de profils détaillés sur les individus, le suivi de leurs activités et de leur interaction avec le gouvernement. Combiné à tout cela est l'attribution à chaque Canadien et Canadienne d'un mécanisme d'authentification, d'identification et d'accès – que le gouvernement désigne comme la « cyberidentité ». Nous pourrions bientôt nous trouver dans une société de surveillance et ne plus avoir droit à la solitude.

LA VIE PRIVÉE DOIT ÊTRE INTÉGRÉE DÈS LE DÉPART À
L'INITIATIVE GOUVERNEMENT EN DIRECT.

De plus, la prestation de services ou le versement de prestations par voie électronique demandera la participation du secteur privé. Les fournisseurs du secteur privé, à titre d'éléments du système de prestation du gouvernement, pourraient devenir des dépositaires de vastes bases de données sur les Canadiens et Canadiennes. Cela est sujet d'inquiétude, compte tenu de la protection restreinte de la vie privée dans le secteur privé, même avec la nouvelle *Loi* qui le vise.

Je me suis adressé à de nombreux auditoires cette année à ce sujet, et j'ai entrepris des consultations continues avec le gouvernement du Canada. Mon message est pourtant simple : la vie privée doit être intégrée dès le départ à l'initiative Gouvernement en direct. Cela comprend la tenue d'évaluations de l'incidence sur la vie privée et la consultation des organismes de protection de la vie privée à l'étape de la conception, et pas en bout de ligne, lorsque les difficultés liées à la vie privée sont déjà ancrées.

Encore une fois, je ne mets pas en question les motifs des responsables de ces initiatives. Il ne fait aucun doute, à mon esprit, que leurs intentions sont les meilleures. L'efficacité est une aspiration louable. Mais, comme je l'ai maintes fois répété, il faut comprendre à juste titre l'efficacité en tant que rapport entre les

moyens et les fins, de façon à choisir les meilleurs moyens pour atteindre des fins précises. Ce qui est critique, c'est la façon de définir ces objectifs. Pour les gouvernements et la société, ces objectifs doivent comprendre la préservation et la protection de la vie privée.

Plus tôt, j'ai brièvement abordé la question des renseignements personnels sur la santé. Il est bien difficile de faire valoir à quel point cette question est importante.

Les gouvernements aux paliers provincial et fédéral ont l'intention d'accroître les activités de collecte et de partage des renseignements médicaux personnels et d'élaborer un système exhaustif de renseignements sur la santé. Leur intention est louable – assurer des soins normalisés et cohérents dans tout le pays, se renseigner sur les causes des maladies, et déterminer qui utilise à bon ou à mauvais escient le système et pourquoi.

Mais, en bout de ligne, le dernier examen médical d'une personne peut potentiellement en viser des milliers d'autres. Et parce que l'état du système de santé représente une préoccupation majeure, les questions touchant la vie privée pourraient être mises de côté, ou du moins n'être abordées que sommairement dans le cadre des discussions.

La perte de contrôle sur les renseignements personnels sur la santé peut comporter des conséquences dévastatrices. Et la crainte de perdre ce contrôle peut inciter certaines personnes à ne pas recourir aux services médicaux. La possibilité d'évaluations psychiatriques détaillées tombant entre les mains d'un administrateur d'assurance ou d'un employeur, par exemple, peut suffire à dissuader des personnes à obtenir des soins. Ou elles peuvent ne pas communiquer des renseignements vitaux à leur médecin, ce qui minerait l'efficacité des traitements et, en fin de compte, gaspillerait les ressources du système de soins de santé.

Dans un récent sondage aux États-Unis, près de 87 % des médecins ont indiqué qu'un patient leur avait demandé de ne pas ajouter certains renseignements à leur dossier. Près de 78 % ont dit qu'ils n'avaient pas versé ces renseignements au dossier, en raison de préoccupations relatives à la vie privée. Il faut se demander si des attitudes semblables sont courantes au Canada.

Concernant un patient donné, les renseignements sur sa santé sont fondamentalement personnels et délicats. Il faut leur assurer le niveau de protection le plus élevé pour que ceux-ci ne soient jamais utilisés au détriment de l'individu auquel ils se rapportent.

Je suis très inquiet au sujet de la sécurité des renseignements médicaux personnels de nature délicate. Le stockage électronique des dossiers médicaux peut non seulement accroître les violations isolées à la vie privée, mais aussi les violations en règle. Nous avons tous entendu parler de communications involontaires de renseignements personnels sur la santé et des manquements à la sécurité sur Internet.

Qu'on pense à l'exemple récent de la communication non autorisée par Eli Lilly de 700 adresses électroniques de personnes qui prenaient l'antidépresseur Prozac. Eli Lilly avait offert aux patients, qui prenaient ce médicament, un service de rappel par courrier électronique. La violation de la vie privée s'est produite lorsqu'un message électronique transmis à la fin de juin et annonçant la fin du programme, comprenait les adresses électroniques des personnes qui s'étaient inscrites au service. Cette seule action a suscité beaucoup de publicité négative pour l'entreprise et a alimenté le débat aux États-Unis au sujet de la difficulté d'assurer la protection des dossiers des patients qui sont archivés électroniquement.

Nous avons également pris connaissance de cas de pirates qui ont eu accès à des dossiers médicaux. En décembre 2000, le *Washington Post* a signalé qu'un pirate hollandais s'était introduit dans le système des dossiers de

LA VIE PRIVÉE N'EST PAS UNE OPTION, PAS PLUS QU'UNE FRIVOLITÉ.
C'EST UN DROIT FONDAMENTAL.

patients à l'University of Washington Medical Center, de Seattle. Le pirate avait téléchargé plusieurs milliers de dossiers qui renfermaient le nom, la condition médicale, l'adresse domiciliaire et le numéro de sécurité sociale des patients. Au pays, le *Vancouver Sun* indiquait, en août, que cinq pharmaciens de la Colombie-Britannique avaient récemment été frappés de sanctions disciplinaires et d'amendes par le Collège des pharmaciens de la province pour avoir indûment pris connaissance des dossiers sur les médicaments de collègues, de parents, d'amis ou de connaissances.

Sommes-nous prêts, en tant que société, à faire face aux manquements à la vie privée et à la sécurité qui peuvent se réaliser? Sans doute, au bas mot, nous devrions demander aux patients s'ils veulent que leurs dossiers médicaux au complet soient stockés sur des supports électroniques. Nous reconnaissons que les dossiers électroniques des patients représentent une autre occasion d'améliorer la qualité des soins. Mais nous devons en même temps reconnaître que ces dossiers peuvent susciter des difficultés liées à la vie privée des patients et à la confidentialité de leurs renseignements. On ne peut donner suite à cette possibilité si nous ne pouvons relever les défis.

En effet, ce seul fait – que les possibilités d'avenir ne peuvent être réalisées de façon satisfaisante sans relever le défi que présente la protection de la vie privée – concerne toutes les questions avec lesquelles j'ai affaire et que j'ai abordées dans le présent compte rendu.

La vie privée n'est pas une option, pas plus qu'une frivolité. C'est un droit fondamental. La nécessité de respecter ce droit tient à l'essentiel de nos espoirs de progrès en tant que société et qu'individus, car tout progrès important vise avant tout à accroître notre qualité de vie. Et nous ne devons jamais nous bercer d'illusions que nous pouvons réaliser une telle amélioration si nous l'envisageons, dans quelque domaine que ce soit, en sacrifiant étourdiment le droit à la vie privée, qui est essentiel à notre liberté et à notre dignité.

Il nous faut combattre cette illusion là où elle se présente et ne pas faire ce sacrifice lorsqu'on tente de nous l'imposer, voilà les visées propres au Commissariat. Dans les parties suivantes du rapport, je rendrai compte des façons dont nous nous sommes acquittés de nos responsabilités.



PREMIÈRE PARTIE

RAPPORT

CONCERNANT

LA *LOI SUR LA*

PROTECTION DES

RENSEIGNEMENTS

PERSONNELS

INTRODUCTION

La *Loi sur la protection des renseignements personnels* assure la protection de la vie privée des individus pour ce qui est des renseignements personnels détenus par les institutions fédérales.

La *Loi*, qui est entrée en vigueur en 1983, régit les moyens pris par les institutions fédérales pour recueillir, utiliser, communiquer et retirer des renseignements personnels, et accorde aux individus le droit d'accéder à leurs renseignements personnels et de demander des corrections au besoin. La *Loi* établit également mes devoirs et responsabilités ainsi que mon mandat.

À titre de Commissaire à la protection de la vie privée, je reçois des plaintes d'individus qui croient que leurs droits aux termes de la *Loi* ont été violés et je fais enquête sur ces plaintes. Je peux également prendre l'initiative d'une plainte et faire enquête moi-même concernant toute situation pour laquelle j'ai des motifs raisonnables de croire que la *Loi* a été violée.

Je suis d'abord avant tout un ombudsman, et je tâche dans la mesure du possible de régler les plaintes par la médiation et la négociation. Mais je possède également de vastes pouvoirs d'enquête qui me sont conférés par la *Loi*. En tant que Commissaire à la protection de la vie privée, je peux contraindre des témoins à comparaître et à témoigner, par exemple, et je peux pénétrer dans des locaux afin d'obtenir des documents et tenir des entrevues.

L'entrave aux enquêtes est une infraction à la *Loi*. Je ne peux toutefois pas contraindre à la conformité avec la *Loi sur la protection des renseignements personnels*, mais je peux recommander des changements à la manière dont les institutions fédérales traitent les renseignements personnels et qui découlent des conclusions de mes enquêtes.

Suivant mon mandat en tant que Commissaire à la protection de la vie privée, je peux également effectuer des vérifications périodiques dans les institutions fédérales afin de déterminer leur niveau de conformité avec la *Loi sur la protection des renseignements personnels* et, sur la base de mes conclusions d'enquête, je peux recommander des changements.

Aux termes de la *Loi*, je suis tenu de déposer un rapport annuel au Parlement sur les activités de l'exercice antérieur du Commissariat. Le présent rapport vise la période du 1^{er} avril 2000 au 31 mars 2001.

ENQUÊTES

La Direction des enquêtes et demandes de renseignements mène des enquêtes sur les plaintes déposées par des individus aux termes de l'article 29 de la *Loi sur la protection des renseignements personnels* (et aux termes de l'article 11 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, dont il sera question ci-après dans le présent rapport).

Par le biais de ces enquêtes, je détermine si les droits à la vie privée des individus ont été violés ou si ces derniers ont pu avoir accès de façon convenable à leurs renseignements personnels. Lorsque les droits à la vie privée d'individus ont été violés, je leur offre des moyens de recours et j'envisage des façons pour empêcher que les violations se reproduisent.

Je suis également autorisé aux termes de la *Loi* à faire prêter serment, à recevoir les éléments de preuve et à entrer dans des locaux. Je peux également examiner ou me faire remettre des copies de documents trouvés dans n'importe quel local.

Jusqu'à présent, toutes les plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels* ont été réglées sans que nous ayons dû invoquer ces pouvoirs d'enquête officiels, parce qu'on a fait preuve de collaboration volontaire lors des enquêtes.

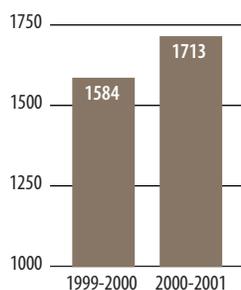
La Direction a également répondu à des milliers de demandes de renseignements du grand public, qui communique avec le Commissariat pour demander des conseils et de l'aide sur toutes sortes de questions touchant la vie privée.

PLAINTES EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Du 1^{er} avril 2000 au 31 mars 2001, nous avons reçu au total 1 713 plaintes en vertu de la *Loi sur la protection des renseignements personnels*,

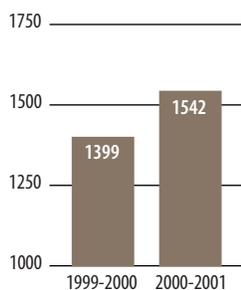
Nombre de plaintes reçues

1^{er} avril 2000 - 31 mars 2001



Enquêtes sur les plaintes terminées

1^{er} avril 2000 - 31 mars 2001



ce qui représente une augmentation de près de 10 % par rapport à l'an dernier. Les genres de plaintes que nous avons reçues concordent également à la tendance établie, c.-à-d. 60 % d'entre elles concernaient soit l'accès refusé aux renseignements personnels soit des questions touchant la collecte, l'utilisation, la communication et le retrait des renseignements personnels, et les 40 % restantes visaient le non-respect des échéances par des organismes fédéraux, qui n'avaient pas donné réponse à une demande de communication de renseignements personnels dans le délai de 30 jours établi dans la *Loi*.

Mon personnel a mené à terme 1 542 enquêtes, autre augmentation de 10 % depuis l'an dernier. Parmi les affaires réglées, 339 touchaient des questions de collecte, d'utilisation, de communication ou de retrait, tandis que 630 se rapportaient à l'accès et 573, aux délais. Les décisions relativement aux plaintes ont été rendues comme suit :

Non fondées :	421
Fondées :	553
Fondées et résolues :	82
Résolues :	44
Résolues en cours d'enquête :	321
Abandonnées :	121

Les plaintes déposées au sujet de ministères qui ne répondent pas aux demandes d'accès dans les délais impartis sont toujours trou-

blantes, car justice différée est justice refusée, et les délais fixés dans la *Loi* l'ont été pour de bonnes raisons.

Plusieurs institutions du gouvernement fédéral se distinguent par le fait qu'il leur arrive trop souvent de ne pas répondre dans les délais prescrits aux demandes d'accès aux renseignements personnels que leur adressent des individus. Il s'agit du Service correctionnel du Canada, du ministère de la Défense nationale, de l'Agence des douanes et du revenu du Canada et de Développement des ressources humaines Canada.

Il m'apparaît de la plus haute importance que tous les ministères et organismes de l'État respectent rigoureusement les délais fixés par la *Loi sur la protection des renseignements personnels*. Le respect des droits que la loi confère aux Canadiens et Canadiennes est obligatoire, et non pas discrétionnaire. Aucune entité du gouvernement du Canada n'a d'excuse pour violer une loi du Canada, et j'entends bien continuer d'insister sur ce point.

Service correctionnel du Canada

À l'automne 2000, compte tenu du nombre de plaintes de non-respect des délais dont a fait l'objet le Service correctionnel du Canada, j'ai chargé mon personnel d'examiner la question avec les cadres supérieurs du SCC.

En février 2001, la Commissaire du Service correctionnel a convenu de mettre en œuvre certaines mesures pour éliminer l'arriéré de demandes dans son Ministère.

Ces mesures ont entraîné une amélioration du traitement des plaintes d'accès au Service correctionnel. En mars 2001, le Ministère avait en cours de traitement 1 684 demandes actives d'accès, dont il avait respecté le délai prescrit de réponse dans seulement environ 20 % des cas. Le 31 août 2001, après une injection de personnel et d'heures supplémentaires, le Ministère a réussi à ramener à 501 le nombre de demandes actives. Près de 60 % de ces demandes ont eu une réponse dans le délai prescrit, et 30 % étaient en retard de 30 jours ou moins.

Certes, il s'agit-là d'une amélioration, et, le 1^{er} juillet, j'ai félicité la Commissaire du Service correctionnel pour la réalisation de son ministère. Le Service correctionnel continue de s'employer à réduire le nombre de demandes en instance et d'abrégier son temps de réponse. Je m'en réjouis, mais cela ne me rend pas euphorique. Rien de moins ne serait acceptable.

Ministère de la Défense nationale

Le personnel du Commissariat a commencé à examiner la question des délais de réponse avec les fonctionnaires du ministère de la Défense nationale à la fin de 1999. À l'époque, le Ministère avait environ 2 100 demandes d'accès en instance. La grande majorité n'avaient pas été traitées dans le délai prescrit. Sur les instances de mes fonctionnaires, le Ministère a convenu de prendre des mesures comme l'embauche de personnel supplémentaire, le travail en heures supplémentaires et la restructuration de ses procédures et de son organisation internes.

Ces efforts ont porté fruit. En novembre 2001, le Ministère avait ramené à 279 le nombre de demandes d'accès en instance. Un peu moins de la moitié, soit 136, n'étaient pas traitées dans les délais prescrits.

Ces chiffres traduisent une amélioration, mais la situation demeure inacceptable. Je reconnais que, pour l'essentiel, les demandes ont trait à de gros dossiers de renseignements concernant des choses comme les enquêtes policières, les commissions d'enquête, ou les plaintes de harcèlement. Le traitement de ces plaintes est difficile. Mais cela doit être un défi, et non pas une excuse.

Agence des douanes et du revenu du Canada

L'Agence a eu d'importantes difficultés à respecter les délais de réponse aux demandes d'accès. Le personnel du Commissariat s'est réuni avec les représentants de l'Agence au début de 2000, tout comme il l'avait fait avec le ministère de la Défense nationale. L'Agence, tout comme la Défense nationale, a accepté de prendre des mesures, comme la réorganisation et l'embauche de nouveau personnel, pour améliorer la situation.

Dans les deux exercices qui ont précédé l'exercice en cours, le Commissariat a reçu 81 plaintes de non-respect des délais la première année, et 127 l'année suivante. La quasi-totalité (95 % la première année, 99 % l'année suivante) ont été jugées fondées.

Pendant l'exercice en cours, le Commissariat n'a reçu que 61 plaintes de non-respect des délais, dont 51 étaient fondées.

Bien que meilleurs que ceux des deux années précédentes, ces chiffres demeurent élevés. Encore une fois, les retards sont probablement le reflet de la complexité des plaintes au sujet des renseignements personnels des dossiers d'impôt, mais il reste des améliorations à apporter.

Développement des ressources humaines Canada

Nous avons reçu 80 plaintes contre Développement des ressources humaines Canada au sujet du non-respect des délais. Près de 60 %, c'est-à-dire 47, concernaient l'accès aux renseignements personnels du Fichier longitudinal sur la main-d'œuvre, le « superfichier » sur les Canadiens et Canadiennes qui a été démantelé l'an dernier à cause de problèmes de protection des renseignements personnels. Il s'agissait d'une situation exceptionnelle, compte tenu de toute l'attention que le dossier a retenue dans les médias et au Parlement, et du grand volume de demandes d'accès que le Ministère a dû traiter. Si l'on fait abstraction de ces circonstances exceptionnelles, il ne nous reste 33 plaintes au sujet des retards de réponse aux demandes d'accès. Ce nombre est encore trop élevé. Mais, compte tenu du nombre de demandes que le Ministère reçoit chaque année, et compte tenu de la taille de ce ministère, le nombre est assez faible pour permettre de croire qu'il suffirait d'un peu de réorganisation et de travail supplémentaire pour l'éliminer. Le Ministère doit s'y employer.

Le Commissariat continuera de surveiller les questions relatives aux délais et mettra de la pression pour qu'il y ait des améliorations continues.

DÉFINITIONS AUX TERMES DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Non fondée : Lorsqu'une plainte est jugée non fondée, cela signifie que l'enquête n'a relevé aucun élément de preuve qui me porte à conclure que l'institution fédérale a violé les droits d'un plaignant aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée : Lorsqu'une plainte est jugée fondée, cela signifie que l'institution fédérale n'a pas respecté les droits d'un individu en vertu de la *Loi sur la protection des renseignements personnels*. Ce serait également ma conclusion dans une situation où l'institution fédérale refuse d'accorder l'accès à des renseignements personnels malgré ma recommandation que ceux-ci soient communiqués. En pareil cas, la prochaine étape consiste à demander un recours en révision à la Cour fédérale du Canada.

Fondée et résolue : Je conclus qu'une plainte est fondée et réglée lorsque les allégations sont corroborées par l'enquête et que l'institution fédérale a accepté volontairement de prendre des mesures correctives pour remédier à la situation.

Résolue : Il s'agit d'une conclusion officielle qui reflète mon rôle d'ombudsman. Cette conclusion est réservée aux plaintes pour lesquelles une conclusion « fondée » serait trop sévère dans les cas de mauvaise communication ou de malentendu. Cela signifie que le Commissariat, après avoir mené une enquête complète et minutieuse, a permis de négocier une solution qui satisfait toutes les parties.

Résolue en cours d'enquête : Il ne s'agit pas d'une conclusion officielle, mais d'une façon acceptable de régler une plainte. Une fois que l'enquête est terminée, le plaignant est satisfait des efforts déployés par le Commissariat et il consent à laisser tomber l'affaire.

Le plaignant retient toutefois le droit de demander qu'une conclusion officielle soit rendue. Le cas échéant, l'enquêteur rouvre le dossier et dépose un rapport officiel. Je dois alors faire rapport sur les conclusions dans une lettre au plaignant.

Abandonnée : Il s'agit d'une enquête qui est terminée avant que toutes les allégations soient pleinement examinées. Une affaire peut être *abandonnée* pour un nombre de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, qui sont essentiels pour en arriver à une conclusion. Je ne dépose pas de conclusion officielle lorsqu'une plainte est abandonnée.

SOMMAIRE DE CAS CHOISIS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Des renseignements personnels trouvés dans un conteneur à ordures au MDN

Dans cette affaire, des dossiers remplis de renseignements personnels ont été trouvés dans un conteneur à ordures à l'extérieur d'un manège militaire. Les dossiers renfermaient des renseignements personnels sur des douzaines d'employés du ministère de la Défense nationale (MDN), y compris leurs nom, adresse et numéro de téléphone personnels, date de naissance, renseignements médicaux et dentaires, des formulaires de vérification de sécurité, des antécédents professionnels, des formulaires d'avis au plus proche parent, des évaluations du rendement, et bien d'autres encore.

Ces renseignements, s'ils avaient été communiqués, auraient pu causer de sérieux préjudices et assurément un embarras personnel et professionnel considérable.

La personne qui a trouvé les dossiers, un réserviste, a signalé la découverte aux officiers supérieurs, mais aucune mesure n'a été prise. Il a été capable d'extraire du conteneur ce qu'il a décrit comme un petit pourcentage des dossiers avant que le conteneur ne soit déversé au dépotoir local comme d'habitude. Il a transmis les dossiers au Commissariat et a

déposé une plainte, alléguant que ses renseignements personnels avaient été retirés de façon indue.

Mon enquête a permis d'établir qu'un bureau devait être réinstallé à un autre étage et, pour préparer le déménagement, on avait ordonné de procéder au retrait de tout ce qui n'était pas nécessaire dans le nouvel emplacement. Le bureau tenait des dossiers parallèles ou « en double » à l'extérieur de la pièce où les dossiers officiels du MDN étaient conservés. Certains des renseignements dans ces dossiers parallèles étaient des doubles de dossiers officiels, tandis que d'autres ne l'étaient pas. Ces dossiers étaient placés dans des chemises ordinaires, qui ne portaient pas le logo du Ministère. Comme ils ne semblaient pas être importants de l'extérieur, personne n'a pensé à en examiner le contenu, et ils ont tout simplement été jetés aux ordures.

Un nombre de dossiers officiels du MDN, qui comprenaient des rapports d'étape sur des candidats renfermant des renseignements personnels détaillés, se trouvaient avec ces dossiers ordinaires.

Les fonctionnaires du MDN ont réagi rapidement, assurant au Commissariat qu'ils prendraient des mesures pour que cela ne se reproduise plus. Le MDN a également accepté de verser les renseignements trouvés dans les dossiers récupérés aux dossiers officiels du Ministère.

Bien que l'usage de « dossiers en double » ne contrevienne pas à la *Loi sur la protection des renseignements personnels*, cette pratique m'inquiète beaucoup. Maintes fois le Commissariat a trouvé des renseignements personnels conservés dans de tels dossiers à de nombreux ministères fédéraux. Il arrive souvent que les renseignements qu'ils renferment ne sont pas communiqués aux individus qui demandent accès en vertu de la *Loi sur la protection des renseignements personnels*, car ceux-ci ne sont pas conservés dans les « dossiers officiels ».

Une question qui a été soulevée au cours de l'enquête a porté sur les lignes directrices relatives au retrait de renseignements personnels du Conseil du Trésor du Canada.

Ces lignes directrices décrivent trois niveaux de renseignements personnels. Le niveau supérieur comprend les renseignements personnels qui, s'ils étaient compromis, « entraîneraient un préjudice extrêmement grave ». Le niveau intermédiaire entraînerait « un préjudice sérieux » si les renseignements étaient compromis. Selon les lignes directrices, il est recommandé de déchiqueter les renseignements personnels de ces niveaux.

Le niveau inférieur comprend les renseignements personnels de nature « peu délicate » qui, s'ils étaient compromis, « causeraient un préjudice ».

Conformément aux lignes directrices, les documents renfermant des renseignements personnels peuvent être déchirés en deux et jetés dans les conteneurs à ordures ordinaires.

Je m'oppose vigoureusement à ces lignes directrices ainsi qu'à leurs dispositions cavaliers visant le retrait des renseignements qui, tel qu'il y est reconnu, pourrait causer un préjudice. En outre, je ne reconnais pas la validité de la distinction entre un « préjudice » et un « préjudice grave ». Lorsqu'il est question de vie privée, tout préjudice est grave. La seule façon acceptable de détruire n'importe quel genre de renseignements personnels est de les déchiqueter.

Le MDN n'est pas la seule institution fédérale à suivre ces lignes directrices. Mes discussions avec les agents de sécurité du MDN sur cette affaire se poursuivent.

Des renseignements personnels détruits de façon prématurée à DRHC

Mon enquête suivant cette plainte m'a permis de conclure que Développement des ressources humaines Canada (DRHC) avait violé à la fois de la *Loi sur la protection des renseignements personnels* et son propre Guide sur les politiques.

Un prestataire d'assurance-emploi s'est plaint au Commissariat que sa capacité d'obtenir tous les renseignements dont il avait besoin pour interjeter un appel avait été entravée par

la destruction par DRHC d'une audiocassette de l'audience initiale relative à son cas devant le Conseil arbitral.

Le Guide sur les politiques de DRHC précise que les cassettes doivent être « conservées pendant une période maximale d'un an ou jusqu'à ce que le cas ait été entendu par (le bureau de) l'arbitre, la Cour fédérale ou la Cour suprême, ainsi qu'en prévision d'une nouvelle enquête par le Conseil arbitral, les arbitres, etc ». Le plaignant avait obtenu deux audiences auprès du Conseil arbitral et avait comparu devant trois arbitres (juges à la Cour fédérale), mais n'avait pas épuisé tous les niveaux d'appel et était prêt à présenter son cas à la Cour fédérale et à la Cour suprême. Ainsi, conformément à la politique de DRHC, l'audiocassette n'aurait pas dû être détruite.

De plus, le *Règlement sur la protection des renseignements personnels* exige des institutions fédérales qu'elles conservent les renseignements personnels utilisés pour prendre une décision administrative pendant une période d'au moins deux ans, pour que l'individu concerné puisse y avoir accès.

Par suite de mon enquête, DRHC a convenu de modifier son Guide sur les politiques, de façon à prévoir une période de conservation de deux ans des audiocassettes utilisées lors d'audiences devant le Conseil arbitral. Il a également modifié le Guide pour renseigner le personnel sur l'obligation de conserver les renseignements personnels pendant une

période de deux ans après les audiences à tous les niveaux juridictionnels, y compris la Cour suprême. Une instruction à cet effet a été envoyée au personnel et la Division des appels a fait paraître une modification du Guide sur les politiques.

Statistique Canada :
préoccupations concernant la publication de renseignements sur certains groupes

Cette plainte a soulevé l'intéressante question de la « protection des renseignements collectifs », et dénote la nécessité de faire preuve de prudence au moment de publier des renseignements sur des groupes identifiables. Bien que les communications de ce genre puissent ne pas permettre d'identifier un individu en particulier, elles comportent toutefois une incidence sur la vie privée car les renseignements sur le groupe peuvent porter atteinte à la vie privée de chaque individu dans le groupe.

Dans ce cas particulier, un homme qui avait été sollicité plusieurs fois au téléphone par des sociétés de courtage a déposé une plainte à l'endroit de Statistique Canada, alléguant que Statistique Canada avait communiqué un nombre important de ses renseignements personnels, obtenus auprès de l'Agence des douanes et du revenu du Canada, pour permettre à une société de recherche de déterminer son revenu annuel.

L'enquête a révélé que les renseignements vendus par Statistique Canada à la société de recherche avaient de fait été tirés du Recensement de 1991 et non des dossiers d'impôt sur le revenu, comme l'avait allégué le plaignant. Et même si les renseignements se rapportaient à une région géographique donnée, ils n'étaient pas organisés selon le code postal, comme l'avait cru le plaignant. En outre, les renseignements ne concernaient pas des individus identifiables ou n'étaient pas de nature personnelle, tels que définis dans la *Loi sur la protection des renseignements personnels*.

Bref, Statistique Canada n'a pas contrevenu à la *Loi sur la protection des renseignements personnels*. Toutefois, la plainte a soulevé une importante question touchant la vie privée des membres de groupes identifiables.

Les produits et services de recensement, même ceux fondés sur des renseignements recueillis auprès d'un échantillon aléatoire de la population de 20 %, peuvent fournir des données suffisamment exactes et détaillées sur les caractéristiques d'une population dans une région géographique donnée. Les sociétés de recherche peuvent assembler des renseignements obtenus de Statistique Canada, ce qu'elles font, sur la base des renseignements tirés d'autres sources, telles que les annuaires téléphoniques et les enquêtes auprès de consommateurs, pour dresser le profil de régions particulières.

Lorsqu'elles peuvent identifier un groupe relativement homogène dans une région géographique donnée, les sociétés de marketing peuvent cibler des individus dans le groupe, les sollicitant pour divers motifs, allant des services financiers à des œuvres de bienfaisance.

Les dommages potentiels dépassent largement les simples inconvénients. Qu'on pense aux effets possibles d'une étude statistique menée dans un petit quartier qui a un taux élevé de troubles mentaux, par exemple, ou d'une étude sur un groupe identifiable dont le taux d'infection au VIH est élevé.

J'ai soulevé mes réserves à ce sujet auprès de Statistique Canada, qui m'a répondu que bien qu'il fasse tout en son pouvoir pour s'assurer que les individus ne peuvent être identifiés dans l'une ou l'autre de ses publications statistiques, il a établi un groupe de travail visant à déterminer les mesures à prendre pour aborder justement les questions touchant la protection des renseignements collectifs. Statistique Canada a signifié sa volonté de collaborer avec mon personnel pour explorer cette question plus avant. Je me réjouis de poursuivre plus amplement des discussions avec Statistique Canada sur cette question.

Un nouveau système électronique à la Défense nationale a compromis la vie privée de milliers de personnes

Le fait de ne pas avoir pris en considération l'incidence sur la vie privée d'un nouveau système électronique d'information a entraîné l'accès possible par n'importe quel employé du ministère de la Défense nationale (MDN) aux renseignements personnels de milliers de membres du personnel militaire. Cette situation aurait pu être évitée si des mesures de sécurité simples avaient été en place.

Ce cas est un exemple classique de la facilité avec laquelle la vie privée peut être compromise même avec de bonnes intentions d'accroître l'efficacité de la gestion.

Le MDN voulait donner aux gestionnaires un outil qui leur permettrait de gérer leur personnel plus efficacement. Toutefois, les agents de projet n'ont pas consulté le coordonnateur de la protection des renseignements personnels du Ministère afin d'assurer que le système était conforme aux exigences de la *Loi sur la protection des renseignements personnels*.

Par conséquent, n'importe quel employé du MDN pouvait visiter le site des ressources humaines sur le réseau informatique interne du Ministère et lire ou télécharger des renseignements personnels détaillés sur les membres des Forces canadiennes. Les renseignements comprenaient la date et le lieu de naissance, l'adresse personnelle, l'état matrimonial, les

noms et dates de naissance des personnes à charge, ainsi que les résultats d'épreuves de compétence linguistique.

Suivant l'intervention du Commissariat, le MDN a accepté de prendre des mesures correctives pour mettre fin à cet accès injustifié. Il a déplacé les renseignements sur un site accessible par mot de passe seulement, et les mots de passe ont été accordés suivant le principe de l'accès sélectif.

Le MDN a également affiché un message électronique sur le site des ressources humaines demandant aux utilisateurs de supprimer tout renseignement tiré de l'ancien site. Je m'inquiétais à l'idée que ce message ne joindrait pas toutes les personnes qui avaient extrait ou téléchargé des renseignements personnels de l'ancien site. J'ai donc demandé au MDN de prendre une mesure corrective supplémentaire pour relever tous les utilisateurs. Le sous-ministre adjoint, Finances et services du Ministère, a envoyé une note de service à tous les cadres supérieurs de la Défense nationale leur demandant d'avertir les employés de supprimer les renseignements personnels tirés du site des ressources humaines initial.

Il est clair, dans cette affaire, que le MDN a contrevenu aux dispositions relatives à l'utilisation et à la communication des renseignements personnels énoncées aux articles 7 et 8 de la *Loi sur la protection des renseignements personnels* et qu'il a violé le droit fondamental

des employés touchant la protection de leurs renseignements personnels. Ainsi, j'ai conclu que cette plainte était fondée. Étant que le MDN a pris des mesures correctives satisfaisantes pour respecter les exigences de la *Loi sur la protection des renseignements personnels*, je considère la plainte comme résolue.

Santé Canada ne sait pas si elle a communiqué des renseignements personnels

Un individu s'est plaint qu'un médecin à Santé Canada a indûment envoyé une évaluation psychiatrique à son sujet à son employeur, l'Agence des douanes et du revenu du Canada (ADRC). ADRC lui a demandé de se soumettre à l'évaluation de la santé et d'aptitude au travail que Santé Canada effectue pour le compte des ministères et agences fédéraux. Pour appuyer son allégation, il a fait référence à une feuille d'accompagnement de télécopie indiquant que Santé Canada avait transmis une télécopie de 11 pages à un conseiller en ressources humaines d'ADRC en octobre 1998.

Une vérification des dossiers de Santé Canada a confirmé que le médecin de Santé Canada avait de fait transmis un document de 11 pages par télécopieur à l'employeur à ce temps-là. Toutefois, l'évaluation psychiatrique du plaignant n'a pas été trouvée dans les dossiers de l'employeur. Il a été impossible de déterminer exactement ce que Santé Canada avait transmis à l'employeur ou même si la télécopie était parvenue à destination.

Si l'enquête avait confirmé que les évaluations avaient été envoyées à l'employeur, j'aurais alors exigé d'étudier les détails de la divulgation. Mon examen aurait consisté à déterminer si la divulgation était conforme aux exigences de la *Loi sur la protection des renseignements personnels*.

À mon avis, il s'agit ici d'un sérieux problème de gestion des dossiers car une institution fédérale chargée d'assurer la protection des renseignements médicaux de nature délicate n'a pu déterminer quels documents ont été transmis par télécopieur ou même si ceux-ci ont été envoyés au bon destinataire.

Pour éviter que ce problème ne se reproduise, Santé Canada a envoyé une note à tous les directeurs dans les bureaux régionaux leur rappelant que les rapports médicaux ne doivent pas être transmis par télécopieur. Dans les cas où les documents doivent être transmis par télécopieur, Santé Canada a établi un protocole à suivre afin d'assurer la protection des renseignements personnels. Le protocole prévoit les mesures suivantes :

- Le nom et le numéro de téléphone du destinataire doivent être indiqués;
- Les documents télécopiés doivent être énumérés sur la feuille d'accompagnement;
- Il faut communiquer avec le destinataire par téléphone avant d'envoyer la télécopie pour assurer que celui-ci est sur place pour recevoir les documents; et

- Le destinataire doit confirmer par écrit la réception des documents.

Ces principes doivent être respectés par toute institution qui transmet des renseignements personnels par télécopieur non sécurisé.

Des renseignements sur des permis de petite embarcation utilisés pour évaluer les taxes de vente

Un homme sur la côte ouest a acheté un petit bateau et a obtenu un permis de petite embarcation auprès d'agents de l'Agence des douanes et du revenu du Canada. Il s'est plaint que l'Agence avait partagé les renseignements sur sa demande de permis avec le ministère des Finances de la Colombie-Britannique, qui a par la suite perçu les taxes de vente provinciales sur le prix d'achat de l'embarcation. Le plaignant a affirmé qu'il ne croyait pas que les propriétaires de nouveau bateau savaient que leurs renseignements personnels étaient communiqués de cette façon.

Bien que les agents des douanes délivrent des permis de petite embarcation, ils le font pour le compte du ministère des Pêches et Océans, qui administre le *Règlement sur les petits bâtiments*, aux termes de la *Loi sur la marine marchande du Canada*.

La compétence du ministère des Pêches et Océans relative à la communication de renseignements personnels sans consentement préalable est conférée aux termes d'une entente entre les gouvernements du Canada

et de la Colombie-Britannique, qui prévoit l'accès, l'utilisation et la communication de renseignements personnels afin d'administrer ou d'appliquer les lois. Cette pratique est conforme aux dispositions de la *Loi sur la protection des renseignements personnels*. C'est pourquoi j'ai conclu qu'il s'agissait d'une communication autorisée de renseignements personnels sans consentement préalable.

J'ai toutefois émis certaines réserves au sujet de la transparence de la collecte de ces renseignements. Le ministère des Pêches et Océans a accepté volontiers de modifier le processus de demande de permis de façon à informer les personnes qui achètent des embarcations que leurs renseignements seront transmis aux provinces aux fins de l'évaluation des taxes de vente. Le Ministère a également convenu de revoir l'entente afin d'en préciser le libellé.

Absence de normes touchant la communication de renseignements personnels aux médecins

Un individu s'est plaint que son employeur, l'Agence des douanes et du revenu du Canada, ait communiqué de ses renseignements personnels en trop grand nombre à un psychiatre.

L'individu en question avait présenté une demande à la Commission de la santé et sécurité au travail du Québec concernant un congé pour des motifs de stress, qui découlait présumément du milieu de travail défavorable

créé par l'employeur. L'employeur, en retour, a contesté la demande de l'employé et demandé l'avis d'un psychiatre par le biais de Santé Canada.

L'employeur a écrit au psychiatre expliquant ses réserves au sujet de l'employé et a joint à la lettre une évaluation du rendement, que l'employé avait refusé de signer, afin d'appuyer ses prétentions. Le plaignant a soutenu que l'évaluation négative n'aurait pas dû être communiquée, et il a caractérisé cette communication comme une tentative par son employeur d'influencer l'avis du psychiatre.

Selon le Protocole d'évaluation de la santé et d'aptitude au travail de Santé Canada, l'employeur doit fournir au médecin la description du problème et les motifs de sa demande d'évaluation. Toutefois le Protocole ne comprend aucune mention concernant l'envoi de documents.

La Politique sur la santé et la sécurité au travail du Conseil du Trésor du Canada ne précise pas le genre de documents à remettre aux médecins. Pas plus qu'Info Source, répertoire des fonds de renseignements personnels au fédéral et le principal outil de référence en place pour aider le public à exercer ses droits aux termes de la *Loi sur la protection des renseignements personnels*. Info Source n'aborde pas la question du recours aux évaluations aux fins des congés de maladie ou d'avis médical. Cela signifie que les gestionnaires au fédéral

n'ont pas de directives sur lesquelles s'appuyer lorsqu'ils transmettent des documents aux médecins qui effectuent l'évaluation d'employés. Il s'agit d'une situation inacceptable.

À la suite des discussions entre le Commissariat et les représentants du Conseil du Trésor et de Santé Canada, le Conseil du Trésor a convenu de réviser sa Norme relative aux examens de santé, de façon qu'elle comprenne les directives suivantes :

- L'employeur doit transmettre une lettre explicative seulement au médecin.
- L'employeur doit consulter le médecin avant de transmettre des documents à l'appui.
- L'employeur ne doit ni utiliser ni communiquer les renseignements personnels de tiers lorsqu'il précise les motifs de sa demande d'évaluation.
- Lorsque la situation le permet, l'employeur doit rencontrer l'employé pour lui expliquer les motifs de la demande d'avis médical et l'informer des renseignements qui seront fournis au médecin et les raisons connexes, de façon à assurer la transparence du processus.
- L'employeur ne doit ni utiliser ni communiquer des renseignements non appuyés de documents, tels que des renseignements sur la foi d'autrui ou des commentaires d'évaluation.

Le Conseil du Trésor a également indiqué qu'il inclura ces directives dans les bulletins qu'il prépare à l'intention des coordonnateurs de l'accès à l'information et de la protection des renseignements personnels qui travaillent dans les organismes fédéraux visés par la *Loi sur la protection des renseignements personnels*.

Les renseignements personnels d'un revendicateur du statut de réfugié communiqués à un autre revendicateur

Un avocat d'immigration s'est plaint que la Commission de l'immigration et du statut de réfugié du Canada ait communiqué des renseignements personnels d'un revendicateur du statut de réfugié à un autre revendicateur. Ce qui est intéressant dans ce cas, c'est que l'avocat représentait indépendamment les deux clients. La Commission lui a donné le Formulaire de renseignements personnels de la femme, qui l'a complété au point d'entrée pour appuyer sa revendication de statut de réfugié, à titre d'avocat-conseil de son ex-conjoint lors des processus d'audience.

Les deux individus s'étaient présentés ensemble au point d'entrée et avaient indiqué à ce moment-là qu'ils étaient conjoints de fait. La Commission a soutenu que les détails qu'ils avaient tous deux fournis dans leur revendication étaient pertinents et servaient à évaluer non seulement leur crédibilité personnelle, mais également celle de leur

conjoint. La Commission a soutenu que l'utilisation des renseignements personnels dans les deux revendications était conforme aux fins initiales pour lesquelles les renseignements avaient été recueillis, c'est-à-dire évaluer leurs revendications respectives de statut de réfugié. J'ai convenu et conclu que la plainte n'était pas fondée.

Néanmoins, ce cas a soulevé d'importantes questions. L'avocat-conseil a fait état de préoccupations concernant les femmes, particulièrement celles victimes de mauvais traitements, dont la revendication du statut de réfugié se fait conjointement à celle d'autres membres de la famille. Il pourrait en découler qu'une femme communique des détails de nature délicate et intime sur les mauvais traitements infligés en salle d'audience où se trouvent de nombreux parents ou anciens parents. Cette expérience pourrait être difficile, voire traumatisante, et porter atteinte à la vie privée d'un individu.

Le processus en vigueur à la Commission prévoit de dispositions dans de telles circonstances. Les revendicateurs peuvent présenter une demande pour que les revendications soient traitées séparément. Je me réjouis d'apprendre que dans cette affaire la Commission a retiré le Formulaire de renseignements personnels rempli par la femme lorsque son avocat s'y est opposé.

Il y aura amélioration apporté au Formulaire de renseignements personnels avec l'ajout d'un paragraphe qui avertit clairement les revendicateurs du statut de réfugié de l'utilisation possible de leurs renseignements personnels lors d'une autre audience.

Jurys de sélection et notes manuscrites

La *Loi sur la protection des renseignements personnels* énonce clairement que les renseignements personnels utilisés par une institution fédérale en vue de prendre une décision administrative au sujet d'un individu doivent être mis à la disposition de cet individu et être conservés pour une période minimale de deux ans.

Cette disposition s'applique aux notes manuscrites que les membres du jury de sélection prennent durant les entrevues pour combler un poste. Les membres du jury de sélection écrivent leurs notes au moment de prendre une décision concernant l'admissibilité à un poste d'un individu en particulier. Cela signifie que les notes ont été utilisées à des fins administratives et doivent être conservées pendant au moins deux ans. Cette question a été abordée dans plusieurs rapports déposés par mon prédécesseur.

Dans cette affaire, un candidat qui n'a pas été retenu pour un poste à Pêches et Océans Canada a demandé d'avoir accès aux notes

manuscrites d'origine qu'avaient prises les membres du jury de sélection afin de préparer un appel touchant le concours. Le Ministère a répondu à sa demande en lui fournissant un exemplaire du rapport sommaire dactylographié des notes des membres du jury, en précisant que les notes d'origine avaient été détruites une fois le concours terminé.

Après délibération, le Ministère a reconnu le bien-fondé de mon opinion, à savoir qu'il lui incombe de conserver dans ses dossiers l'original des notes. Des fonctionnaires du Ministère ont affirmé qu'ils n'ont pas délibérément refusé l'accès aux renseignements personnels et m'ont assuré que les politiques avaient été modifiées de façon que les notes d'origine des membres du jury de sélection sont conservées dans les dossiers de dotation.

Le courrier électronique personnel n'est pas nécessairement privé

Un employé du ministère de la Défense nationale (MDN) s'est demandé si son employeur était autorisé à utiliser et à communiquer ses messages électroniques privés dans une enquête visant une plainte de harcèlement, alors que ces messages électroniques avaient été indûment recueillis.

Une personne avait eu accès à l'ordinateur du plaignant et avait téléchargé bon nombre de ses messages électroniques. Ceux-ci renfermaient des renseignements personnels

sur le plaignant ainsi que des commentaires dérogatoires au sujet de collègues. Les messages ont été imprimés et laissés sur le bureau de plusieurs employés. Après avoir lu ces messages, les employés en cause en ont donné copie à leur supérieur et ont déposé une plainte de harcèlement contre le plaignant.

L'employeur a retenu les services d'un consultant pour enquêter sur les plaintes de harcèlement et lui a remis copie des messages électroniques qui lui servirait de preuve pour appuyer son enquête. (Une enquête distincte n'a pas permis de déterminer qui avait téléchargé les messages.)

Lorsque le plaignant a appris que ses messages électroniques avaient été remis au consultant, il s'est plaint au Commissariat en affirmant qu'ils avaient été obtenus de façon inconvenante en premier lieu et que l'employeur n'avait pas le droit de s'en servir dans l'enquête sur les plaintes de harcèlement ou de les remettre au consultant.

Cette affaire a soulevé des questions importantes et opportunes. Bien qu'il ne s'agisse pas d'une enquête criminelle, cette situation porte toutefois à réfléchir sur l'utilisation, lors d'une enquête, d'éléments de preuve qui ont été obtenus de façon injuste, douteuse et possiblement illicite.

Cela soulève la question générale de la surveillance en milieu de travail et particulièrement

le respect de la confidentialité des communications électroniques, dossier chaud ces dernières années. Comme je l'ai mentionné plus tôt dans le présent rapport, les employeurs soutiennent souvent que la surveillance des communications électroniques est justifiée en raison de la nécessité de protéger les employés contre le harcèlement.

Je crois fermement que les employeurs doivent assurer une telle protection. Mais je ne crois pas que cette protection se traduise nécessairement par la surveillance générale des communications électroniques ou de l'utilisation des ordinateurs. Il faut accepter qu'il y a des limites contraignantes au droit d'un employeur de lire le courrier des employés ou d'écouter leurs conversations téléphoniques ou vider leurs tiroirs. Je crois qu'il faut regarder de près les communications électroniques afin de déterminer les principes à appliquer à leur sujet.

La *Politique d'utilisation des réseaux électroniques* du Conseil du Trésor du Canada repose sur le postulat que la *Charte des droits et libertés* assure la protection de la vie privée des employés. Elle prévoit que les institutions mettent en place leur propre politique sur l'usage des réseaux électroniques. Elle précise également que la politique doit établir les usages autorisés et acceptables des réseaux. La politique du Conseil du Trésor n'interdit pas la surveillance dans certaines conditions particulières.

La politique du MDN sur la gestion du courrier électronique précise que les employés ne peuvent s'attendre au respect de leur vie privée lorsqu'ils utilisent les systèmes de courrier électronique. Je trouve cela particulièrement déplorable. La loi en matière de la protection de la vie privée a été élaborée en se fondant sur la notion d'« attentes raisonnables de respect de la vie privée », et l'une des façons dont les tribunaux déterminent s'il y a eu violation de la vie privée est d'établir tout d'abord si une personne peut raisonnablement s'attendre à ce que sa vie privée soit respectée à un endroit et à un moment donnés. Mais je ne suis pas d'accord qu'en raison de ce principe on porte atteinte à la vie privée d'un employé ou de quiconque en lui disant simplement qu'il ne peut s'attendre au respect de celle-ci. Bien que la gestion ait le droit et la responsabilité de gérer, elle doit toutefois le faire en tenant compte de certaines contraintes, y compris le respect des droits fondamentaux. Il ne revient pas à la direction seulement de déterminer si l'attente en matière de respect de la vie privée est raisonnable.

Dans cette affaire, j'ai conclu que l'employeur n'avait pas contrevenu aux dispositions de la *Loi sur la protection des renseignements personnels*, et, ce qui est peut-être plus important, qu'il n'avait pas agi de façon déraisonnable dans les circonstances. Je crois que l'attente au respect de la vie privée du

plaignant ne pouvait être satisfaite lorsque ses messages électroniques se sont retrouvés entre les mains de ses collègues. La façon dont cela s'est produit, à tort ou à raison, n'est pas en cause ici, et je n'ai trouvé aucune preuve que le gestionnaire ou supérieur du plaignant a surveillé son courrier électronique ou qu'il a indûment eu accès au courrier.

L'employeur était autorisé à embaucher un consultant pour mener l'enquête sur les plaintes de harcèlement, et j'ai conclu qu'il avait le droit de remettre les messages électroniques au consultant. Comme les plaintes reposaient sur ces messages, l'employeur n'aurait raisonnablement pu refuser de les donner au consultant.

Enfin, j'ai informé le plaignant que les employés qui se servent du réseau électronique de l'employeur de façon qui contrevient à la politique ministérielle – dans la présente affaire, écrire des messages dérogoatoires au sujet de collègues, ce qui peut être perçu comme une forme de harcèlement – ne peuvent s'attendre à ce que leurs supérieurs ignorent ce comportement inconvenant lorsque celui-ci est porté à leur attention. De nouveau, la façon dont on a renseigné le supérieur à ce sujet n'est pas en cause. S'il avait été démontré que les gestionnaires ou les supérieurs avaient de fait accédé au courrier électronique du plaignant, il se peut fort bien que j'aurais perçu cette affaire différemment.

INCIDENTS VISÉS PAR LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Un incident est une affaire qui est portée à mon attention et qui doit faire l'objet d'une enquête, sans toutefois constituer une plainte officielle en vertu de la *Loi sur la protection des renseignements personnels*. Durant la période visée par le présent rapport, nous avons examiné 21 incidents dont j'ai eu connaissance de diverses sources. La majorité de ces incidents concernaient la communication par inadvertance de renseignements personnels ou de présumées violations à la *Loi sur la protection des renseignements personnels*. Les exemples les plus frappants sont présentés dans les lignes qui suivent.

L'ouverture du courrier – le droit à la vie privée doit être la première considération

En mars 2001, il a été révélé que des fonctionnaires de l'Agence canadienne des douanes ouvraient du courrier qui arrivait au Canada et qu'ils transmettaient les renseignements à Citoyenneté et Immigration Canada. Le caractère sacré de la correspondance personnelle est une pierre angulaire de la vie privée, et les Canadiens et Canadiennes s'attendent à ce que le courrier soit seulement ouvert par le destinataire prévu. Nous n'habitons pas un pays où les autorités ouvrent couramment le courrier, ou du moins c'est ce que nous croyions. Je me suis immédiatement penché sur cette affaire.

De nombreuses personnes étaient surprises d'apprendre que l'ouverture du courrier par un agent des douanes était licite, dans la mesure où l'envoi postal pèse plus de 30 grammes. Si le courrier pèse moins de 30 grammes, la *Loi sur les douanes* interdit de l'ouvrir, à moins d'avoir un mandat de perquisition ou le consentement du destinataire. Mais dans la mesure où le courrier pèse plus de 30 grammes, qu'il s'agit d'un colis ou de correspondance personnelle, les inspecteurs des douanes peuvent l'ouvrir s'ils croient qu'il contient des articles de contrebande ou de faux documents. Tout envoi considéré suspect du point de vue de l'immigration est remis aux agents d'immigration aux fins d'examen et de mesures ultérieures.

J'ai de sérieuses réserves au sujet de cette distinction arbitraire et artificielle en matière de poids, qui permet d'ouvrir non seulement des colis mais aussi la correspondance privée. Celle-ci doit être traitée avec le plus grand respect de façon à protéger la vie privée. Le poids de la correspondance ne devrait pas faire de différence. Pour envoyer une lettre par « messagerie prioritaire », il faut la mettre dans une grande enveloppe plutôt lourde, qui souvent fait que l'article entre dans la catégorie « de plus de 30 grammes ». Une lettre reste une lettre et la protection des renseignements qu'elle contient doit être assurée même lorsque l'expéditeur choisit un mode de livraison rapide et sûr ou que celle-ci est plus volumineuse et lourde.

J'ai indiqué mes réserves à ce sujet à la ministre de Citoyenneté et Immigration, et j'ai fait les recommandations suivantes :

- Lorsque les agents des douanes découvrent un objet solide et qui semble ne pas être de la correspondance dans une enveloppe pesant plus de 30 grammes, le fait de l'ouvrir est considéré comme une activité habituelle du processus en vigueur à l'Agence des douanes.
- Lorsque les agents ne trouvent pas d'objet solide et que l'enveloppe est retenue seulement parce qu'ils soupçonnent qu'elle peut contenir des documents frauduleux, l'Agence des douanes doit remettre le courrier sans l'ouvrir au représentant d'Immigration. Ce dernier peut alors obtenir un mandat pour l'ouvrir s'il a des motifs raisonnables de le faire.

La ministre de Citoyenneté et Immigration a rejeté ces recommandations, indiquant la difficulté apparente à constater la présence d'objets solides, comme des cartes laminées dans des enveloppes, ainsi qu'en raison du fort volume de courrier acheminé par les centres postaux. Essentiellement, elle a soutenu que la mise en œuvre des recommandations exigerait beaucoup plus de ressources.

Parce qu'il m'a été impossible d'en arriver à un consensus avec la ministre de Citoyenneté et Immigration, je me suis adressé au ministre responsable de l'Agence des douanes et du revenu du Canada. Mes entretiens avec le ministre du Revenu national ont porté fruit. L'Agence a modifié ses politiques et ne tient pas compte à présent du poids des enveloppes de type courrier à savoir si l'envoi postal pèse plus ou moins de 30 grammes. Les lettres à l'intérieur des colis sont traitées comme du courrier personnel et ne sont pas ouvertes si ces lettres pèsent moins de 30 grammes. J'ai grandement apprécié l'aide du ministre du Revenu national pour résoudre cette affaire.

Santé Canada et sa liste de présumés utilisateurs de marijuana

Santé Canada a communiqué avec le Commissariat après avoir reçu l'appel d'une journaliste qui disait avoir obtenu les noms de 128 individus qui avaient présenté une demande au Ministère afin d'être exemptés en vue de se procurer de la marijuana à des fins médicales.

Mon enquête a porté sur deux questions : déterminer quelles étaient le nom des personnes sur la liste de façon à les aviser que leurs renseignements personnels avaient été compromis, et savoir comment la journaliste avait obtenu cette liste.

La journaliste a refusé de remettre la liste au Commissariat ou à Santé Canada. Comme plus de 160 personnes avaient fait une demande pour l'exemption relative à la marijuana lorsque cette affaire a été révélée, il était impossible de déterminer l'identité des 128 personnes sur la liste de la journaliste. Santé Canada n'a pas eu le choix et a dû informer tous les individus du fait qu'elle n'avait pas protégé leurs renseignements personnels.

Afin d'identifier la source de la fuite, Santé Canada a mené une enquête à l'interne. Elle a trouvé que sa sécurité était inadéquate. Presque tous les employés du Bureau de substances contrôlées avaient eu accès aux noms sur la liste. Les recommandations en vue d'améliorer la sécurité ont été mises en œuvre rapidement. Maintenant, la base de données est visée par un accès sélectif et son utilisation est restreinte par mot de passe.

En ce qui concerne la liste même, suivant l'intervention du Commissariat, la journaliste a convenu de la détruire. La liste n'a pas été publiée et la journaliste a confirmé qu'elle n'en avait pas fait de copie.

J'ai été satisfait des mesures de sécurité mises en œuvre par Santé Canada et de ses efforts pour sensibiliser les employés à leurs obligations aux termes de la *Loi sur la protection des renseignements personnels*.

Vol de demandes remplies de permis d'armes à feu à Justice Canada

Dans le cadre de ses efforts pour promouvoir l'enregistrement des armes à feu, le Centre canadien des armes à feu de Justice Canada offre un programme d'extension, afin de joindre les propriétaires d'armes à feu dans leur collectivité. Par le biais de services dans les centres commerciaux et de cliniques mobiles qui se rendent dans les petites villes et les foires rurales, le personnel aide les gens à remplir une demande de permis d'armes à feu et poste les formulaires remplis à un centre de traitement des permis. En Colombie-Britannique, une des cliniques mobiles a été volée. Celle-ci a été retrouvée, mais la boîte qui contenait quelque 20 demandes remplies manquait.

À la suite de reportages dans les médias sur cet incident, j'ai demandé qu'on fasse enquête sur les circonstances du vol ainsi que sur les efforts déployés par le Centre pour identifier et aviser les demandeurs dont les formulaires manquaient. Non seulement des renseignements personnels avaient disparu, mais des individus malhonnêtes pouvaient se servir de ces renseignements pour obtenir des permis d'armes à feu auxquels ils n'avaient pas droit.

Le Centre a lancé un appel dans les médias aux individus qui avaient rempli une demande durant les jours qui ont précédé le

vol pour qu'ils se fassent connaître. Seulement deux l'ont fait. Nous espérons que d'autres demandeurs communiqueront avec le Centre lorsqu'ils tarderont à obtenir leur permis. Par mesure de protection à long terme, le Centre a mis à jour sa politique pour assurer que les demandes remplies sont postées au Centre canadien des armes à feu en fin de journée. Bien que cet incident ne soit toujours pas réglé, je suis satisfait des efforts déployés par le Centre pour tâcher de réparer sa bévue.

Des préoccupations au sujet d'une technologie d'identification biométrique

La technologie biométrique, qui identifie les personnes suivant leurs caractéristiques physiques, est d'intérêt spécial pour le Commissariat. Lorsque les médias ont signalé que la GRC se servait d'un logiciel de reconnaissance de visage pour surveiller les voyageurs à l'Aéroport Pearson de Toronto et pour identifier des criminels, j'ai immédiatement lancé une enquête.

Il a toutefois été révélé que ce reportage était erroné. La GRC n'utilise pas des caméras de surveillance équipées d'un dispositif d'identification biométrique, bien que le logiciel soit utilisé dans les centres de détention de la GRC à l'aéroport pour analyser les photos d'individus qui ont été arrêtés. La photo d'un

individu qui a été arrêté est prise par une caméra numérique puis archivée sur le disque dur d'un ordinateur autonome. Le logiciel mesure point-à-point l'ossature du visage et compare la photo numérique de l'individu arrêté aux photos qui sont déjà stockées dans le système. Comme l'ossature ne peut être modifiée au même titre que la couleur des cheveux ou des yeux, le système permet de reconnaître les individus qui ont plusieurs identités. Essentiellement, il s'agit d'une version perfectionnée des traditionnelles photos de criminels utilisées par les forces de l'ordre.

Dans les circonstances, j'étais convaincu que le logiciel d'identification biométrique n'était pas utilisé, comme l'avaient signalé les médias, et aucune question en matière de vie privée n'a été soulevée.

Une contribuable a reçu le remboursement d'une autre personne

Une bonne idée de nouvelle est tombée entre les mains d'une journaliste du *Calgary Herald* lorsqu'elle a reçu la cotisation d'impôt sur le revenu et le remboursement d'une autre personne dans la même enveloppe que les siens.

Une enquête du Commissariat a déterminé qu'une erreur mécanique au Centre de production de Winnipeg de Travaux publics et Services gouvernementaux Canada était la

cause. Le Centre de production de Winnipeg imprime et poste les cotisations fiscales ainsi que les chèques pour le compte de l'Agence des douanes et du revenu du Canada.

Le centre est pleinement automatisé pour imprimer, couper et plier les cotisations et les chèques. Les documents sont placés dans des enveloppes, qui sont scellées. Les enveloppes ensuite scellées sont lues par un détecteur optique qui les transperce au faisceau lumineux. Un avertisseur est déclenché lorsqu'une enveloppe est trop épaisse.

Cette année toutefois, en raison de changements dans la qualité du papier utilisé et le nombre d'exemplaires du formulaire, les enveloppes sont plus épaisses. Le détecteur optique n'a pu être adapté pour tenir compte de ces changements et il était inopérable.

Seulement un incident de ce genre a été signalé. Afin d'assurer que cela ne se reproduise pas, le Centre a amélioré son processus de contrôle de la qualité et a accru l'échantillonnage aléatoire des produits finals.

J'étais satisfait des mesures prises par Travaux publics pour prévenir des erreurs futures et qu'il ait présenté des excuses à l'individu concerné.

COMMUNICATIONS DANS L'INTÉRÊT PUBLIC

Aux termes de l'alinéa 8(2)m) de la *Loi sur la protection des renseignements personnels*, le dirigeant d'un ministère peut communiquer des renseignements personnels sans le consentement de l'individu lorsque l'intérêt public contraignant l'emporte sur l'atteinte à la vie privée d'un individu ou lorsque la communication est à l'avantage de l'individu. L'« intérêt public contraignant » concerne souvent une question de sécurité et de sûreté publiques, ou l'obligation des ministères de rendre compte au public des décisions qu'ils ont prises.

Les dirigeants des ministères sont tenus, aux termes du paragraphe 8(5) de la *Loi*, de m'aviser par écrit de tout recours à cette disposition. Idéalement, ils le font avant la communication des renseignements. Le cas échéant, je peux aviser l'individu concerné de la divulgation des renseignements. Dans tous les cas, je veille à ce que seuls les renseignements personnels nécessaires soient communiqués de façon à atteindre l'objectif d'intérêt public visé.

Durant la période visée par le présent rapport annuel, on m'a avisé de 53 cas de ces communications.

L'an dernier, la majorité des avis me sont parvenus de la GRC, de la Défense nationale, du Service correctionnel Canada et de la Commission nationale des libérations conditionnelles.

La GRC a fait un nombre de communications dans l'intérêt public concernant la libération de délinquants sexuels dans la collectivité lorsque ceux-ci avaient purgé leur peine. Dans la majorité des cas, les délits sexuels avaient été commis à l'endroit d'enfants, et les délinquants présentaient des risques élevés de récidive. Certains étaient même considérés comme des délinquants sexuels dangereux. En raison des préoccupations à l'endroit des citoyens dans les collectivités où les délinquants ont été libérés, la GRC était d'avis que la communication au public des renseignements personnels sur ces délinquants compensait les préjudices causés par l'atteinte à la vie privée de ces derniers.

À plusieurs reprises, la Défense nationale a communiqué des renseignements relatifs au décès de membres en exercice des Forces canadiennes. Les renseignements ont été communiqués aux plus proches parents pour des motifs de compassion, en espérant qu'une meilleure compréhension des circonstances entourant le décès de leurs proches les aiderait à vivre leur deuil.

Service correctionnel du Canada et la Commission nationale des libérations conditionnelles ont fait paraître un nombre de rapports de la Commission d'enquête touchant des questions telles que les évasions d'établissements fédéraux, la violation des conditions de la libération d'office, et la récidive de délinquants, y compris le meurtre, une fois libérés. Ces rapports comprenaient des renseignements personnels. La majorité des cas ont beaucoup retenu l'attention des médias. Les individus ont été réincarcérés, mais en raison de la couverture médiatique et de l'attention du public, Service correctionnel du Canada et la Commission nationale des libérations conditionnelles étaient d'avis qu'il était dans l'intérêt du public de communiquer ces rapports. Ces communications étaient perçues comme nécessaires pour que le public puisse comprendre les événements entourant les incidents et les mesures prises pour empêcher qu'ils se reproduisent.

Dix premiers ministères selon le nombre de plaintes reçues*1^{er} avril 2000 - 31 mars 2001*

Organisation	Total	Accès aux renseignements personnels	Délais	Atteinte à la vie privée	Autre
Service correctionnel du Canada	672	136	342	194	
Agence des douanes et du revenu du Canada	197	91	59	47	
Développement des ressources humaines Canada	190	63	88	39	
Gendarmerie royale du Canada	136	85	24	26	1
Défense nationale	100	40	46	14	
Citoyenneté et Immigration Canada	90	32	48	10	
Centre canadien du renseignement de sécurité	40	37	2	1	
Société Postes Canada	38	16	4	18	
Justice Canada	30	8	12	10	
Affaires étrangères et Commerce international Canada	27	4	23	0	
Autres	193	97	42	54	
Total	1 713	609	690	413	1

Enquêtes terminées et résultats selon le ministère ou l'organisme

1^{er} avril 2000 - 31 mars 2001

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Agriculture et Agroalimentaire Canada	0	0	0	0	0	5	5
Bureau du vérificateur général du Canada	1	0	1	0	0	0	2
Agence des douanes et du revenu du Canada	64	15	57	6	28	60	230
Société canadienne d'hypothèques et de logement	0	0	0	0	0	1	1
Société canadienne des ports	0	0	0	2	0	0	2
Société Postes Canada	5	1	5	0	2	11	24
Agence canadienne d'évaluation environnementale	0	0	0	0	0	1	1
Agence canadienne d'inspection des aliments	0	0	0	1	0	2	3
Commission canadienne des grains	0	0	0	1	0	0	1
Patrimoine canadien	0	0	1	0	0	3	4
Service canadien du renseignement de sécurité	0	2	43	0	0	2	47
Bureau du directeur général des élections	0	0	0	1	0	2	3
Citoyenneté et Immigration Canada	35	7	21	7	0	12	82
Commissariat aux langues officielles	0	0	0	1	0	0	1
Service correctionnel du Canada	262	23	59	48	2	63	457
Environnement Canada	0	0	0	0	0	4	4
Finances Canada	1	0	0	0	0	0	1
Pêches et Océans Canada	0	0	1	0	0	1	2

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1^{er} avril 2000 - 31 mars 2001

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Affaires étrangères et Commerce international Canada	3	0	4	1	1	3	12
Santé Canada	5	0	26	1	1	2	35
Développement des ressources humaines Canada	79	4	21	14	2	37	157
Commission de l'immigration et du statut de réfugié du Canada	4	3	6	0	0	2	15
Affaires indiennes et du Nord canadien	4	0	2	0	0	5	11
Industrie Canada	0	0	5	1	0	3	9
Justice Canada	2	0	43	3	0	8	56
Bureau du Canada pour le millénaire	0	0	1	0	0	0	1
Archives nationales du Canada	1	0	7	6	2	12	28
Défense nationale	55	13	26	7	1	26	128
Commission nationale des libérations conditionnelles	1	0	3	0	0	7	11
Conseil national de recherches Canada	0	0	2	0	0	0	2
Ressources naturelles Canada	0	0	0	0	1	0	1
Bureau de l'ombudsman, Défense nationale et Forces canadiennes	1	0	0	0	0	3	4
Commission d'appels des pensions	0	0	0	0	0	1	1
Bureau du Conseil privé	0	0	3	1	0	1	5
Commission de la fonction publique du Canada	1	1	3	1	0	0	6
Commission des relations de travail dans la fonction publique	0	1	5	0	0	0	6

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1^{er} avril 2000 - 31 mars 2001

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Travaux publics et Services gouvernementaux Canada	8	0	6	1	0	2	17
Commission des plaintes du public contre la GRC	0	1	1	0	0	0	2
Gendarmerie royale du Canada	18	9	51	12	4	25	119
Conseil de recherches en sciences humaines du Canada	0	0	0	0	0	1	1
Bureau du solliciteur général du Canada	0	2	11	1	0	0	14
Statistique Canada	1	0	1	0	0	0	2
Transports Canada	2	0	0	1	0	3	6
Conseil du Trésor du Canada	0	0	3	1	0	0	4
Administration portuaire de Vancouver	0	0	0	2	0	0	2
Anciens combattants Canada	0	0	3	1	0	13	17
Total	553	82	421	121	44	321	1 542

Enquêtes terminées selon les motifs et les résultats

1^{er} avril 2000 - 31 mars 2001

	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Accès aux renseignements personnels	11	73	241	54	36	215	630
Accès	11	70	229	51	15	207	583
Correction-annotation	0	3	12	3	21	5	44
Langue	0	0	0	0	0	1	1
Frais inexacts	0	0	0	0	0	2	2
Atteinte à la vie privée	45	9	124	58	8	95	339
Collecte	3	0	28	33	2	32	98
Conservation et retrait	2	2	9	0	4	7	24
Utilisation et communication	40	7	87	25	2	56	217
Délais	497	0	56	9	0	11	573
Corrections-délais	15	0	1	1	0	0	17
Délais	473	0	31	8	0	10	522
Avis de prorogation	9	0	24	0	0	1	34
Total	553	82	421	121	44	321	1 542

Lieu d'origine des enquêtes terminées*1^{er} avril 2000 - 31 mars 2001*

Province / Territoire	Nombre
Terre-Neuve	5
Île-du-Prince-Édouard	3
Nouvelle-Écosse	103
Nouveau-Brunswick	50
Québec	306
Région de la capitale nationale – Québec	11
Région de la capitale nationale – Ontario	177
Ontario	347
Manitoba	82
Saskatchewan	63
Alberta	109
Colombie-Britannique	267
Nunavut	0
Territoires du Nord-Ouest	3
Yukon	9
Étranger	7
Total	1 542

Demandes de renseignements par type en vertu de la Loi sur les renseignements personnels*1^{er} avril 2000 - 31 mars 2001*

Sujet	Nombre
Adoption, généalogie, personnes portées disparues	31
Recensement	45
Dossiers criminels, pardons, exonération de l'impôt des É-U	190
E-311 Formulaire de déclaration du voyageur	39
Armes à feu	44
Fichier longitudinal sur la main-d'œuvre	68
Dossiers médicaux	91
Des députés	27
Absence de compétence fédérale	427
<i>Loi sur la protection des renseignements personnels, interprétation et processus</i>	6 460
Affaires publiques (médias et publications)	896
Réacheminées aux commissaires provinciaux	1 068
Réacheminées à une autre agence fédérale	651
Réacheminées à d'autres	499
Registre des électeurs	21
Numéro d'assurance sociale	746
Autres	296
Total	11 599

PRATIQUES EN MATIÈRE DE VIE PRIVÉE ET EXAMENS

Introduction

Aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels*, je suis autorisé à entreprendre, de façon aléatoire, des examens de la conformité relativement aux pratiques de traitement des renseignements personnels des institutions fédérales. Cela signifie que je procède à une vérification afin d'assurer que celles-ci se conforment aux principes qui régissent la collecte, l'utilisation, la communication, la protection, la conservation et le retrait des renseignements personnels, tels qu'établis aux articles 4 à 8 de la *Loi*.

Le Commissariat réalise des examens de la conformité aux termes de l'article 37 depuis 1984. J'ai élargi cette fonction l'an dernier, établissant la Direction des Examens et pratiques en matière de vie privée, qui me permet d'évaluer la mesure dans laquelle les organismes se conforment aux exigences établies dans la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. (La loi visant le secteur privé me confère des pouvoirs semblables en matière de vérification; mes activités de vérification dans le secteur privé sont discutées dans la deuxième partie du présent rapport.)

En tant qu'ombudsman, je préfère que les vérifications de la protection des renseignements personnels soient non conflictuelles, dans la mesure du possible. Idéalement, une vérification constitue une démarche coopérative et constructive qui permet d'aborder des questions avant qu'elles ne deviennent des plaintes. Les vérifications servent aux organisations qui veulent améliorer leurs pratiques de traitement des renseignements personnels. Bien que j'aie les mêmes pouvoirs en ce qui concerne les vérifications que ceux liés aux enquêtes, c'est-à-dire assigner des témoins à comparaître, faire prêter serment, et contraindre les organisations à produire des éléments de preuve, je n'y ai recours que lorsque je n'obtiens pas de collaboration volontaire.

Mon personnel de la Direction des Examens et pratiques en matière de vie privée, en plus de faire des vérifications et des examens, travaille auprès des organismes fédéraux qui cherchent à mieux comprendre les questions relatives à la conformité et les implications de leurs programmes et pratiques sur la vie privée. Il est essentiel que les ministères fédéraux explorent à fond sur la façon dont il faut protéger la vie privée avant de donner suite à leurs plans, même avec les meilleures intentions qui soient, de façon à réduire les coûts et à protéger les citoyens. Sur demande, mon personnel de la Direction étudie les nouvelles propositions de gestion de

renseignements, comme des initiatives de couplage de données, la création de bases de données et les ententes de partage de renseignements avec d'autres organisations. Il s'agit d'une autre façon d'assurer que les droits à la vie privée des Canadiens et Canadiennes sont respectés.

Dans les pages qui suivent, sont décrits trois principaux cas touchant les pratiques de traitement des renseignements personnels d'institutions fédérales.

Des renseignements personnels n'ayant pas été déchiquetés – Golden West Document Shredding, Inc.

J'ai parlé de nombreuses fois de la nécessité d'instituer une « culture de la vie privée » au sein d'organisations, à la fois publiques et privées. Chaque fois que je lis un article dans une revue qui porte sur la vie privée, que je prends connaissance du programme d'une conférence, ou que j'examine le dernier sondage sur les préoccupations touchant la vie privée, l'accent est toujours placé sur le secteur privé. Bien que cet accent soit indiqué, il ne faut pas perdre de vue l'incroyable diversité de renseignements personnels que les gouvernements collectent, utilisent et partagent. En effet, bon nombre des plus sérieuses menaces à la vie privée continuent d'émaner de gouvernements.

À l'opposé des entreprises, les gouvernements ont le pouvoir de demander des renseignements personnels des citoyens. Ils recueillent ces renseignements en application de la *Loi*. Lorsqu'un organisme ou un programme gouvernemental a besoin de renseignements personnels pour donner suite à sa mission, ces renseignements seront recueillis. Les individus n'ont pas le choix dans cette situation.

En tant que citoyens, nous devons interagir avec le gouvernement afin de pouvoir participer aux programmes sociaux, bénéficier de l'aide sociale, et contribuer à l'intérêt public par les régimes fiscaux. Ce faisant, nous confions au gouvernement certains de nos renseignements personnels les plus délicats. Que nous présentions une demande à l'assurance-emploi, produisions nos déclarations de revenus, enregistrons nos armes à feu, ou remplissons les formulaires de recensement, nous ne sommes pas dans une position de force pour nous opposer à la collecte ou à l'utilisation de nos renseignements.

C'est pourquoi le gouvernement doit être particulièrement vigilant en maintenant la confiance que les citoyens accordent à sa capacité d'assurer la sécurité et la confidentialité des dossiers qui documentent leur vie ainsi que leur identité en tant que citoyens canadiens.

Le cas suivant représente un manquement clair à ce mandat public, et montre de façon flagrante ce qui peut arriver lorsque les coûts et la convenance l'emportent sur la vie privée.

Plus de 30 ministères et organismes fédéraux avaient entreposé des dossiers au Centre fédéral de documents de la région du Pacifique des Archives nationales du Canada. Le Centre détenait littéralement des tonnes de renseignements personnels de nature hautement délicate. Suivant la procédure normale, ces dossiers doivent être détruits après la période de conservation établie. Imaginez notre réaction lorsque un journaliste du *Vancouver Sun* nous a avisé qu'une entreprise du secteur privé, dont les services avaient été retenus pour déchiqueter et recycler les dossiers, vendait les documents au plus offrant – *intacts*, parce que du papier intégral rapporte davantage que du papier déchiqueté sur le marché du recyclage.

L'enquête a révélé qu'entre janvier et la mi-juillet 1998, les Archives nationales avaient envoyé plusieurs centaines de tonnes de documents à Golden West Document Shredding, Inc. à Burnaby (C.-B.) pour qu'ils soient détruits. Cela s'ajoutait aux documents que Golden West avait reçus directement d'autres institutions fédérales. La liste partielle suivante énumère certains des genres de dossiers

dont il s'agissait, et montre la mesure dans laquelle la vie privée des Canadiens et Canadiennes peut avoir été compromise :

- de la Division de l'impôt de Revenu Canada, plus de 22 000 boîtes de documents, y compris des déclarations de revenus, des feuillets T4, des relevés de revenus de placement;
- de Développement des ressources humaines Canada, des demandes de prestations d'assurance-emploi, des dossiers de counseling en matière d'emploi de clients, des demandes de la sécurité du revenu et du supplément de revenu garanti;
- de Statistique Canada, des enregistrements d'emploi de recensement, des dossiers d'entrevues de recensement, des enquêtes sur l'emploi et d'autres natures;
- de Travaux publics et Services gouvernementaux Canada, des dossiers de rémunération d'employés, des registres de chèques, et des registres de paie;
- de Citoyenneté et Immigration Canada, des dossiers de cas d'immigration.

Si ces renseignements étaient tombés entre les mauvaises mains, les conséquences auraient été désastreuses pour des milliers de citoyens canadiens. Des renseignements personnels détaillés, comme les numéros d'assurance

sociale, les dates de naissance, les numéros de comptes bancaires et les adresses domiciliaires, représentent des biens valables. En ce qui concerne le crime en prolifération, connu comme le vol d'identité, ces renseignements servent aux criminels pour obtenir des cartes de crédit, ouvrir des comptes bancaires, réacheminer le courrier, louer des véhicules, et même obtenir un emploi. Les victimes du vol d'identité subissent de substantielles pertes de revenu, et doivent déployer beaucoup d'efforts pour rétablir leur solvabilité et leur réputation.

Mon personnel a obtenu des preuves contraignantes que les gestionnaires de Travaux publics et Services gouvernementaux Canada, de même que ceux des Archives nationales étaient au courant des sérieuses difficultés financières, techniques et en matière de sécurité de l'entreprise de déchiquetage, avant de lui accorder une autorisation de sécurité en vue de transporter et de déchiqueter des déchets de papier fédéraux protégés. En outre, l'entreprise qui s'est vu attribuer le marché de déchiquetage n'était même pas la même que celle qui avait présenté la soumission initiale. En effet, la soumission a été présentée par Golden West Document Shredding Inc., entreprise en faillite, et non Golden West Document Shredding (1995) Inc., à qui le

marché a été adjugé. Cette incohérence n'a pas été relevée ou a tout simplement été ignorée.

L'agent de sécurité de Travaux publics qui a inspecté les installations de Golden West a conclu que celles-ci satisfaisaient à peine aux exigences minimales nécessaires afin d'accorder une autorisation de sécurité. Mais il a toutefois accordé cette autorisation après que le gestionnaire du Centre fédéral de documents des Archives nationales l'a assuré que les Archives nationales inspecteraient régulièrement les installations et signaleraient tout problème à Travaux publics.

Les inspections, comme il a été révélé, n'ont pas empêché l'entreprise de vendre les documents protégés non déchiquetés. En juillet 1998, lors d'une visite impromptue des installations de déchiquetage de Golden West, les employés de Travaux publics et des Archives nationales ont trouvé qu'environ 95 tonnes de documents protégés non déchiquetés avaient été vendus à une entreprise de rachat de papier et que ceux-ci avaient été mis en balles et préparés pour être expédiés outre-mer ainsi qu'aux États-Unis aux fins de recyclage.

La GRC a mené une enquête et a fait rapport à Travaux publics, mais le rapport n'a pas été rendu public et le Commissariat n'a pas été avisé de cette situation inquiétante. Des renseignements que nous avons obtenus auprès de la GRC dans le cadre de notre enquête indiquent qu'avant que les documents ne soient saisis de Golden West en juillet 1998, une entreprise de recyclage avait acheté quatre chargements de camion de renseignements gouvernementaux. Deux chargements avaient été expédiés par camion aux États-Unis et deux autres avaient été expédiés outre-mer, dont l'un en Corée du Sud et l'autre en République populaire de Chine. La GRC n'a pu établir si les documents avaient été déchiquetés.

Dans mes conclusions à la suite de l'enquête, j'ai convenu du bien-fondé des constatations de la GRC, c'est-à-dire que la responsabilité de cet incident incombe carrément aux Archives nationales et à Travaux publics. Tous deux n'ont pas pris de précautions convenables en retenant les services de Golden West, et ne se sont pas acquittés de leurs responsabilités qui consistent à protéger les renseignements personnels de nature hautement délicate de milliers de Canadiens et Canadiennes.

Le marché a été adjugé à Golden West après que les Archives nationales ont décidé de supprimer le service interne de destruction de déchets de papier protégés pour les ministères fédéraux. Cette décision a été prise afin de

réduire les coûts, sans toutefois porter suffisamment attention à la protection de la vie privée. Le souci d'économie ne peut avoir préséance sur les obligations légales de protéger les renseignements personnels d'individus. Il incombait pleinement aux Archives nationales, qui agissaient pour le compte d'autres ministères et organismes, d'assurer la sécurité et la confidentialité de tous les renseignements jusqu'à ce que les documents soient déchiquetés. À la fois les Archives nationales et Travaux publics (en sa qualité d'adjudicateur) étaient tenus d'assurer que l'entrepreneur détruise les dossiers de façon indiquée.

Les Archives nationales ont un rôle essentiel à jouer pour assurer que les dossiers protégés du gouvernement sont convenablement détruits à la fin de leur cycle de vie. Elles doivent indiquer la voie à suivre concernant l'établissement de normes et de pratiques relatives à la gestion des dossiers et des renseignements du gouvernement du Canada. Le fait de demander aux ministères de prendre leurs propres arrangements pour éliminer les déchets protégés augmente considérablement les risques. Cet incident ne se serait jamais produit si les Archives nationales avaient continué de déchiqueter les déchets au centre régional de documents ou si les fonctionnaires avaient surveillé en tout temps les opérations de déchiquetage.

Dans une perspective de gestion des risques, la meilleure solution consisterait à rétablir le déchetage des dossiers de nature délicate dans les locaux des Archives nationales. Une solution de rechange consisterait à recourir aux services de déchetage privés de l'extérieur, mais seulement s'ils peuvent garantir des mesures de sécurité convenables, et seulement dans la mesure où le déchetage fait l'objet d'une surveillance constante par le personnel des Archives nationales. Je me rends compte des implications substantielles touchant les ressources associées à ces solutions pour les Archives nationales, et je suis prêt à discuter de toute autre proposition qui s'avérerait aussi efficace.

Suivant les conclusions dans cette enquête, j'ai formulé une série de recommandations aux Archives nationales et à Travaux publics, et je leur ai demandé de présenter un rapport au Commissariat sur les façons envisagées pour donner suite à ces recommandations. Je leur ai également demandé d'informer à l'avenir le Commissariat sans délai relativement à toute communication accidentelle ou incorrecte de renseignements personnels.

De plus, j'ai averti les deux organismes que j'informerai le Conseil du Trésor, qui est chargé d'établir la Politique sur la sécurité du gouvernement du Canada et de veiller à ce que les ministères la respectent, de mes

inquiétudes au sujet de la sécurité et de la confidentialité des renseignements personnels qui doivent être éliminés. Le Conseil est donc convenu d'examiner avec soin les recommandations de mon rapport qui concernent soit la Politique sur la sécurité soit la norme particulière sur la sécurité des contrats dans le contexte de l'examen en cours de la Politique sur la sécurité du gouvernement du Canada, en vue de diminuer les risques qu'un tel incident se reproduise.

Préoccupations en matière de vie privée du Programme canadien des armes à feu

Le Commissariat s'est beaucoup intéressé au Programme canadien des armes à feu depuis la mi-1990 – bien entendu parce que le Programme vise la collecte et l'utilisation de quantités considérables de renseignements personnels de nature hautement délicate. Le Commissariat a cerné un nombre d'inquiétudes potentielles en matière de vie privée lorsque le concept avait initialement été proposé, suggérant plusieurs modifications afin de protéger la vie privée lorsque le projet de loi était à l'étude au Parlement, et donnant des commentaires ultérieurs lorsque le règlement a été annexé aux mesures législatives. Aucune de nos suggestions n'a été retenue.

Le Commissariat continue de recevoir de nombreuses demandes de renseignements et plaintes au sujet du Programme, y compris de députés. Mon prédécesseur a entrepris un examen en janvier 2000 des pratiques de traitement des renseignements personnels du Programme. Cet examen est maintenant terminé. À la lumière de ce qui a été révélé, mes principales préoccupations liées à la vie privée qui touchent le Programme se rapportent à deux domaines : les droits d'accès et de correction, et la collecte et l'utilisation des renseignements personnels.

Le droit d'accès et de correction est très important parce que des renseignements inexacts ou non corroborés dans la base de données Personnes d'intérêt – Armes à feu, par exemple, peuvent entraîner des délais, la non-délivrance de permis, et l'interrogation de voisins ou de connaissances. (La base de données Personnes d'intérêt – Armes à feu a été créée en 1998 afin de satisfaire aux objectifs de l'article 5 de la *Loi sur les armes à feu* touchant l'inadmissibilité à un permis. Plus de 900 organismes d'application de la *Loi* partout au Canada entrent des codes de déclaration d'incidents dans le Réseau du Service national de police, qui servent ensuite d'indicateurs dans la base de données dans le cadre du processus d'examen des demandes.)

Les individus qui veulent exercer leur droit d'accès et de correction de leurs renseignements personnels conservés par le Programme canadien des armes à feu trouvent qu'il est difficile de le faire et ils doivent y consacrer beaucoup de temps. La nature multijuridictionnelle du Programme fait que ces derniers doivent parfois se rendre à plusieurs ministères ou organismes ou à différents paliers de gouvernement pour accéder à leurs renseignements personnels.

Un résidant de l'Ontario, par exemple, où des lois provinciales et municipales sur la vie privée sont en vigueur, peut être tenu de présenter jusqu'à trois demandes d'accès distinctes pour obtenir les renseignements personnels se rapportant à une demande de permis d'armes à feu qui est présentée au palier fédéral. La situation est pire pour les résidents de l'Île-du-Prince-Édouard, qui n'ont toujours pas de droit d'accès autorisé en vertu d'une loi à leurs renseignements personnels détenus au niveau provincial.

Concernant la collecte et l'utilisation des renseignements personnels, mon examen a révélé que les mesures de contrôle limitant l'accès au Système de récupération de renseignements judiciaires, par exemple, sont inadéquates. Les agents aux armes à feu ont

accès à plus de renseignements que ceux dont ils ont besoin pour prendre des décisions concernant l'admissibilité des demandeurs. Ils ont également accès à des renseignements personnels sur d'autres individus, comme des témoins, des connaissances et des victimes. Ces derniers ne présentent pas de demande de permis. Ces renseignements à leur sujet ne seraient normalement pas pertinents suivant les exigences du Programme.

Un autre problème découle du fait que les préposés aux armes à feu se fient aux renseignements recueillis dans le Système de récupération de renseignements judiciaires sans en vérifier l'exactitude auprès du service de police d'origine. Cela est contraire à la fois aux politiques établies de la GRC et au paragraphe 6(2) de la *Loi sur la protection des renseignements personnels*, qui prévoit que les renseignements personnels soient exacts, à jour et complets. L'examen a également révélé que certains des renseignements recueillis dans les bases de données de la police pour le système Personnes d'intérêt – Armes à feu se rapportent à des incidents qui ne sont pas admissibles aux termes de l'article 5 de la *Loi sur les armes à feu* ou qui sont fondés sur des renseignements non corroborés.

J'ai également évalué les questions sur les antécédents personnels du formulaire de demande de permis d'armes à feu afin de déterminer si elles sont conformes aux restrictions de la *Loi sur la protection des renseignements personnels* visant la collecte de renseignements personnels.

À mon avis, le Programme canadien des armes à feu n'a pas démontré la nécessité de toutes les questions. J'ai des réserves au sujet de la nature d'intrusion large de ces trois questions :

- « 19d) : Au cours des cinq dernières années, avez-vous tenté ou menacé de vous suicider ou, après avoir consulté un médecin, avez-vous fait l'objet d'un diagnostic ou subi un traitement à la suite d'une dépression, d'abus d'alcool ou de drogues, de problèmes comportementaux ou émotifs?
- 19e) : Au cours des cinq dernières années, la police ou les services sociaux ont-ils, à votre connaissance, reçu une plainte contre vous pour usage, tentative ou menace de violence ou autre conflit à la maison ou ailleurs?
- 19f) : Au cours des deux dernières années, avez-vous vécu un divorce, une séparation, une rupture d'une relation importante, ou encore avez-vous perdu un emploi ou fait faillite? »

J'ai recommandé que que les questions des paragraphes 19 d) et 19 f) soient éliminées et que celle du paragraphe 19 e) soit modifiée pour éliminer les références telles que « autre conflit » et « ailleurs » afin d'évacuer toute ambiguïté.

Bien que mon examen ait également soulevé certaines questions touchant la communication des renseignements personnels et les mesures de sécurité, il a été révélé que les mesures de sécurité matérielles, personnelles et en matière de technologie de l'information conviennent aux renseignements protégés. Toutefois, l'examen a montré que le Programme canadien des armes à feu n'a toujours pas adopté de politiques, procédures et pratiques touchant la conservation et le retrait des dossiers du Programme.

Suivant cet examen, j'ai formulé 34 recommandations pour que des mesures correctives soient prises concernant les pratiques générales de gestion des renseignements personnels du Programme. Bien que je reçoive des commentaires positifs de la Gendarmerie royale du Canada, je n'ai toujours pas reçu de réponse du ministère de la Justice.

L'examen n'a pas abordé les questions qui ont été soulevées à la suite de la recherche et du travail sur le terrain, sur lequel s'appuie l'examen, y compris les questions d'impartition et les ententes internationales de partage

de renseignements. De plus, l'examen n'a pas porté sur le traitement des renseignements personnels par l'Agence des douanes et du revenu du Canada. Depuis le 1^{er} janvier 2001, l'ADRC est chargée d'administrer la partie de la *Loi sur les armes à feu* qui porte sur les déclarations en douanes et le mouvement des armes à feu. Au moment de l'examen, cette partie de la Loi n'était toujours pas en vigueur. Nous étudions actuellement ces aspects du Programme.

Un nouveau protocole relatif aux bases de données est adopté suivant le Fichier longitudinal sur la main-d'œuvre

Développement des ressources humaines Canada (DRHC) a démantelé le Fichier longitudinal sur la main-d'œuvre en mai 2000, après que le public s'est insurgé contre celui-ci. Depuis, DRHC a mis en œuvre un protocole rigoureux touchant tous les projets de recherche futurs entrepris par l'un ou l'autre de ses bureaux.

Le protocole s'applique à toutes les activités d'analyse, de recherche et d'évaluation qui nécessitent le couplage de bases de données séparées. Il vise également le couplage de données externes, y compris les activités avec un entrepreneur de l'extérieur. Il couvre également l'utilisation d'identificateurs personnels non masqués aux fins d'enquête, que celle-ci soit menée par DRHC, un

entrepreneur ou Statistique Canada et que la source de données soit une base de données interne (c.-à-d. de DRHC) ou externe.

Nonobstant le fait que DRHC réalisera seulement des couplages pour des analyses et recherches en matière de politique, conformément à son mandat établi dans la *Loi*, la principale caractéristique du protocole est d'établir un équilibre. Le protocole s'appuie sur des principes liés à l'intérêt public, y compris la confidentialité, la transparence, l'évaluation de l'intérêt public et l'évitement de préjudices potentiels pour les individus et les groupes identifiables.

Je me réjouis de constater que DRHC a reconnu que le couplage des données entre des bases de données distinctes constitue une intrusion flagrante à la protection de la vie privée. DRHC envisagera seulement de telles entreprises lorsque les avantages sont clairement dans l'intérêt public national. Une autre exigence tient au fait que l'objectif du projet ne doit ni être au détriment des individus concernés ou de groupes identifiables ni que le projet vise à prendre des décisions administratives à leur sujet.

Le protocole prévoit également que la diffusion d'information liée au couplage des données dans les bases soit effectuée conformément aux dispositions sur la confidentialité

de la *Loi sur le ministère Développement des ressources humaines Canada*, la *Loi sur la protection des renseignements personnels*, la *Loi sur l'assurance-emploi*, la *Loi de l'impôt sur le revenu*, le *Régime de pensions du Canada*, et la *Loi sur la sécurité de la vieillesse* ainsi qu'aux critères relatifs à la communication des renseignements compris dans les ententes avec les provinces, les territoires et les autres ministères et organismes fédéraux.

Je suis également très heureux de voir que tous les liens entre les bases de données devront satisfaire à un examen et à un processus d'approbation prescrit, entre autres mesures de protection. Cela comprend la présentation de propositions documentées à un comité de spécialistes à l'interne, le Comité d'examen des banques de données, auquel siègent surtout des hauts fonctionnaires de DRHC. Le processus d'examen prévoit la consultation du Commissariat concernant tous les projets, ainsi que des partenaires à l'extérieur lorsque le projet comporte le couplage des bases de données de DRHC avec des données de l'extérieur. Enfin, la recommandation du Comité d'examen des banques de données a été transmise au sous-ministre de Développement des ressources humaines, qui est chargé d'approuver tous les projets.

DRHC travaille actuellement à l'élaboration d'un cadre de protection juridique qui régira les activités futures de collecte et d'utilisation de données et de renseignements obtenus auprès de Canadiens et Canadiennes, dont se servira DRHC pour ses besoins particuliers en matière de recherche. Le cadre comprendra des sanctions pour les mésusages et sera conforme aux lois, politiques et procédures du fédéral ainsi qu'aux constatations qui découleront de tout examen par le gouvernement de la *Loi sur la protection des renseignements personnels*.

Depuis septembre 2000, nous avons donné des commentaires à DRHC sur plus d'une douzaine de présentations, y compris l'Enquête canadienne par panel sur l'interruption d'emploi, le Programme canadien de prêts aux étudiants – Principales mesures du rendement, et le Programme de prestations d'emploi et de mesures de soutien.

Dans l'ensemble, je suis satisfait que DRHC a abordé les préoccupations que le Commissariat a soulevées concernant le Fichier longitudinal sur la main-d'œuvre dans son protocole de couplage des bases de données et son cadre de protection juridique proposé.

Examens

La Commission de l'immigration et du statut de réfugié et la Commission canadienne de sûreté nucléaire

Les examens des pratiques de traitement des renseignements personnels aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels* ont été entrepris vers la fin du présent exercice à la Commission de l'immigration et du statut de réfugié et à la Commission canadienne de sûreté nucléaire. Ces examens ont compris des visites sur place dans la région de la capitale nationale ainsi que des bureaux régionaux choisis partout au Canada. Les examens seront terminés durant l'exercice 2001-2002.

DEVANT LES TRIBUNAUX

Introduction

La Division juridique, dirigée par l'avocat général, me donne des conseils juridiques et stratégiques spécialisés ainsi qu'un soutien au contentieux touchant la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*, un individu est autorisé, à la suite de mon enquête, à recourir à la Cour fédérale pour

demander la révision de la décision d'une institution fédérale qui lui a refusé l'accès à des renseignements personnels. Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983 jusqu'au 31 mars 2001, 106 demandes de révision avaient été déposées à la Cour fédérale. Six d'entre elles ont été déposées l'exercice dernier.

Je suis autorisé, aux termes de l'article 42 de la *Loi sur la protection des renseignements personnels*, après avoir terminé une enquête, de présenter à la Cour fédérale un recours en révision d'une décision prise par une institution fédérale qui refusé l'accès à des renseignements personnels, dans la mesure où j'ai obtenu le consentement de l'individu qui a initialement demandé l'accès aux renseignements. Trois demandes ont été déposées par les anciens commissaires à la protection de la vie privée de 1984 à la fin de l'exercice 2001.

Les commissaires précédents et moi sommes également intervenus devant les tribunaux six fois au total depuis 1984 jusqu'à présent dans des demandes présentées par d'autres personnes aux termes de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*.

Décisions récentes

Le Commissaire à la protection de la vie privée c. le Conseil canadien des relations de travail

Il s'agit d'un appel interjeté par mon prédécesseur concernant la décision de la Section de première instance de la Cour fédérale. L'affaire portait sur les notes prises par des membres du Conseil canadien des relations de travail lors d'une audience sur une plainte relative au manquement au devoir de juste représentation. Mon prédécesseur a soutenu que les notes, qui contenaient des renseignements personnels du demandeur, relevaient de l'autorité du Conseil et étaient ainsi visées par le droit d'accès prévu dans la *Loi sur la protection des renseignements personnels*.

L'appel a été entendu le 9 mai 2000, et la décision a été rendue à l'audience.

La Cour d'appel fédérale a soutenu que les notes des membres du Conseil n'étaient pas visées par l'autorité du Conseil, tel que prévu à l'alinéa 12(1)b) de la *Loi sur la protection des renseignements personnels*. La Cour a déclaré : « Ces notes sont prises dans le cadre d'une instance quasi judiciaire non pas par des employés du Conseil, mais par des représentants du gouverneur en conseil investis de fonctions juridictionnelles qu'ils doivent exercer, non pas en qualité de mandataires du

Conseil, mais de façon indépendante par rapport aux autres membres de celui-ci, y compris le président dudit Conseil ou d'une institution fédérale. L'absence de contrôle que le Conseil peut exercer sur les notes en qualité d'institution fédérale s'explique principalement par l'application aux tribunaux administratifs du principe de l'indépendance judiciaire et de son corollaire, le principe du privilège décisionnel. »

Mon prédécesseur n'en a pas appelé de cette décision.

Le Commissaire à l'information du Canada (appelant) c. le Commissaire de la GRC (intimé) et le Commissaire à la protection de la vie privée (intervenant)

L'affaire portait sur l'équilibre entre la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*. Une liste des affectations de quatre agents de la GRC avait fait l'objet d'une demande aux termes de la *Loi sur l'accès à l'information*. Le Commissaire de la GRC a refusé de communiquer ces renseignements parce qu'ils se rapportaient aux antécédents professionnels de ces individus et qu'il s'agissait ainsi de renseignements personnels aux termes de l'alinéa 3b) de la *Loi sur la protection des renseignements personnels*. Le Commissaire à l'information a déposé un recours en révision de ce refus devant la Cour.

La question en litige consistait à déterminer si les renseignements pouvaient être communiqués conformément à la définition de « renseignements personnels » à l'alinéa 3j) de la *Loi sur la protection des renseignements personnels*, qui précise que les renseignements touchant les postes ou fonctions d'agents ou d'employés du gouvernement ne constituent pas des renseignements personnels.

La Cour d'appel fédérale a soutenu que les renseignements en litige étaient de fait des renseignements personnels sur chaque agent et qu'ils ne relevaient pas de l'exception prévue à l'alinéa j) de la définition de « renseignements personnels ».

La Cour a rejeté l'argument de la GRC, selon lequel l'exception prévue à l'alinéa j) s'applique seulement au poste qu'occupe actuellement un fonctionnaire (ou au dernier poste occupé dans le cas d'un ancien fonctionnaire). La Cour a convenu du bien-fondé de l'argument du Commissaire à l'information et de moi-même, c.-à-d. que l'alinéa j) peut s'appliquer aux postes antérieurs.

La Cour a rejeté l'argument du Commissaire à l'information, selon lequel il faut adopter une interprétation large de l'exception énoncée à l'alinéa j) pour justifier la communication des renseignements demandés. La Cour a con-

venu du bien-fondé de ma position, indiquant que l'exception devrait être interprétée d'une manière qui ne permet pas la communication des « antécédents professionnels » d'un individu.

Le Commissaire à l'information a été autorisé à interjeter appel de cette décision à la Cour suprême du Canada. Je vais demander l'autorisation d'intervenir dans cet appel.

Affaires en instance

Formulaires de déclaration du voyageur (E-311)

Les deux cas suivants portent sur la communication de renseignements personnels par l'Agence des douanes et du revenu du Canada à la Commission de l'assurance-emploi du Canada aux fins d'un programme d'appariement des données d'enquête. Les renseignements personnels en question ont été tirés de formulaires de déclaration du voyageur (E-311) présentés aux douanes par des résidents canadiens de 1994 à 1996. L'objet de l'appariement des données était d'identifier les prestataires d'assurance-emploi qui touchent des prestations alors qu'ils sont à l'extérieur du Canada. Aux termes de la *Loi sur l'assurance-emploi*, les prestataires doivent être prêts à travailler et ils sont inadmissibles aux prestations s'ils s'absentent du Canada.

Le Commissaire à la protection de la vie privée c. le Procureur général du Canada

Il s'agit d'un appel interjeté à la Cour suprême du Canada touchant une décision de la Cour d'appel fédérale. Les questions en litige consistaient à savoir si la Cour d'appel fédérale a erré en concluant que la communication de « renseignements personnels » par l'Agence des douanes à la Commission de l'assurance-emploi du Canada était autorisée aux termes de l'article 8 de la *Loi sur la protection des renseignements personnels* et de l'article 108 de la *Loi sur les douanes*, à savoir si l'alinéa 108(1)b de la *Loi sur les douanes* autorise le Ministre à communiquer des renseignements personnels à la Commission en vue de leur utilisation dans un programme d'appariement de données d'enquête, et si le ministre a autorisé comme il se doit la communication des renseignements personnels sur les formulaires de déclaration du voyageur à la Commission en vue de leur utilisation dans un programme d'appariement des données d'enquête.

Il s'agit d'un renvoi présentée à la Cour fédérale conjointement par mon prédécesseur et le procureur général du Canada. La Section de première instance de la Cour fédérale a donné raison à mon prédécesseur, mais non la Cour d'appel fédérale.

La Cour d'appel fédérale a rendu sa décision le 9 février 2000 à l'audience. Les principales conclusions sont les suivantes :

- L'appariement des données est autorisé par le protocole d'entente auxiliaire pour la collecte et la communication des renseignements recueillis par l'Agence des douanes sur les voyageurs, entente qu'ont conclue le 26 avril 1997 l'Agence des douanes et la Commission canadienne de l'assurance-emploi du Canada. L'alinéa 108(1)b) de la *Loi sur les douanes* confère au ministre du Revenu le pouvoir discrétionnaire d'autoriser l'entente exposée dans le protocole auxiliaire de 1997. La Cour a statué que l'autorisation antérieure accordée en 1991 par le ministre du Revenu aux termes de l'alinéa 108(1)b) de la *Loi sur les douanes* n'était pas pertinente à l'affaire dont elle était saisie.
- L'alinéa 8(2)b) de la *Loi sur la protection des renseignements personnels* doit être interprété largement. La Cour a déclaré : « Dans ce contexte, on ne peut faire autrement qu'interpréter l'alinéa 8(2)b) comme une disposition permettant au législateur de conférer à tout ministre (par exemple), au moyen d'une loi donnée, un large pouvoir discrétionnaire quant à la forme et au fond relativement à la

communication de renseignements que son ministère a recueillis, ce pouvoir discrétionnaire devant naturellement être exercé conformément à l'objet de la *Loi sur la protection des renseignements personnels*. »

- Ces objectifs ont été atteints parce que le Ministre : « a estimé que la communication demandée par la Commission l'était pour un usage permis et qu'aucun renseignement autre que ceux dont la Commission avait besoin ne serait communiqué ». En outre, le protocole auxiliaire de 1997 comprend des restrictions applicables à l'utilisation des renseignements et à leur communication à des tiers ainsi que d'autres mesures comme l'établissement d'une piste de vérification et la destruction des renseignements.

Contestation en vertu de la Charte

Il s'agit d'un appel interjeté à la Cour suprême du Canada touchant la décision de la Cour d'appel fédérale. Les questions en litige sont :

- À savoir si la communication par l'Agence des douanes à la Commission de l'assurance-emploi du Canada de renseignements personnels tirés des formulaires de déclaration du voyageur et l'utilisation subséquente de ces

renseignements dans un programme d'appariement des données comme élément de preuve contre l'individu contreviennent au droit de l'individu de ne pas faire l'objet de fouille ou de saisie déraisonnable, aux termes de l'article 8 de la *Charte*;

- Et si tel est le cas, à savoir si l'élément de preuve aurait dû être exempté aux termes du paragraphe 24 2) de la *Charte*; et
- À savoir si la disposition de la *Loi sur l'assurance-emploi* qui rend inadmissible aux prestations tout individu qui s'absente du Canada porte atteinte à la liberté de circulation garantie au paragraphe 6(1) de la *Charte*.

La Cour d'appel fédérale a rejeté la demande de contrôle judiciaire de la décision prononcée par le juge-arbitre nommé conformément à la *Loi sur l'assurance-emploi*. La Cour d'appel fédérale, dans une décision prononcée le 9 février 2000, a conclu que les Canadiens et Canadiennes ne peuvent raisonnablement s'attendre au respect de la vie privée touchant les renseignements inscrits sur les formulaires E-311 de manière à susciter l'application de l'article 8 de la *Charte* (droit de ne pas faire

l'objet de fouille, de perquisition ou de saisie déraisonnable). La Cour a aussi statué que l'alinéa 32b) de la *Loi sur l'assurance-chômage* (l'alinéa 32b) de la *Loi sur l'assurance-emploi* : inadmissibilité aux prestations d'assurance-emploi durant une absence du Canada) ne porte pas atteinte à la liberté de circulation garantie aux termes du paragraphe 6(1) de la *Charte*.

État de la situation

Les demandes d'appel à la Cour suprême du Canada des deux décisions ont été accordées le 17 août 2000. Les deux avis d'appel ont été déposés et signifiés le 22 août 2000.

La requête pour énoncer une question constitutionnelle dans le cadre de la contestation en vertu de la *Charte* a été signifiée aux procureurs généraux de chaque province et territoire, comme le prévoit les règles de la Cour suprême du Canada. Les procureurs généraux de l'Ontario, du Manitoba et du Québec sont intervenus.

Les affaires ont été entendues le 7 novembre 2001.

Clayton Charles Ruby
c. le Solliciteur général

Il s'agit d'un appel interjeté à la Cour suprême du Canada touchant une décision de la Cour d'appel fédérale. Le requérant s'est vu refuser l'accès à des renseignements personnels le concernant dans des fichiers par le Service canadien du renseignement de sécurité. Le Solliciteur général a refusé de communiquer les renseignements demandés par le requérant. La Section de première instance de la Cour fédérale a rejeté la demande de révision des décisions de refus. La décision a été portée en appel à la Cour d'appel fédérale où l'appel a été accueilli en partie, et les deux questions ont été renvoyées à la Section de première instance de la Cour d'appel fédérale pour une nouvelle décision.

La Section de première instance de la Cour fédérale, de même que la Cour d'appel fédérale ont examiné la constitutionnalité de l'article 51 de la *Loi sur la protection des renseignements personnels*, qui prévoit le dépôt des renseignements devant la Cour en l'absence de l'autre partie et la tenue d'une audience à huis clos. Les deux instances inférieures ont conclu que l'article 51 de la *Loi sur la protection des renseignements personnels* viole l'alinéa 2b) de la *Charte*, mais que cette violation se justifie au regard de l'article 1 de la *Charte*.

Questions soulevées dans l'appel

- À savoir si l'article 51 de la *Loi sur la protection des renseignements personnels* contrevient à l'article 7 de la *Charte* et, si tel est le cas, cette contravention est justifiée aux termes de l'article 1; et
- À savoir si la violation de l'alinéa 2b) de la *Charte* par l'article 51 de la *Loi sur la protection des renseignements personnels* est justifiée aux termes de l'article 1.

Questions soulevées dans l'appel incident

- À savoir si la Cour d'appel fédérale a interprété l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels* si étroitement que les institutions fédérales seront incapables de protéger convenablement le nom de leurs sources de renseignements, y compris les informateurs de police; et
- À savoir si la Cour d'appel fédérale a négligé de prendre suffisamment compte des implications de l'« effet mosaïque » et de la nécessité d'interpréter les exceptions de la *Loi sur la protection des renseignements personnels* de manière à préserver la capacité du gouvernement de protéger ses sources, ses méthodes et ses techniques d'enquête ainsi que sa capacité de faire exécuter les lois du Canada.

Dans sa décision du 8 juin 2000, la Cour d'appel fédérale a soutenu que l'article 7 de la *Charte* n'était pas en cause car les mesures de protection procédurales prévues à l'article 51 de la *Loi sur la protection des renseignements personnels* ne portaient pas atteinte aux intérêts de liberté des individus. Concernant l'alinéa 2b) de la *Charte*, la Cour d'appel fédérale a soutenu que l'article 51 de la *Loi sur la protection des renseignements personnels* violait le droit de liberté de presse, mais pouvait tout de même être légitimé en tant que limite raisonnable et justifiable aux termes de l'article 1 de la *Charte*.

Une autre question prise en considération par la Cour était l'interprétation convenable de l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels* qui autorise une institution fédérale à refuser l'accès aux renseignements personnels lorsqu'il est raisonnable de s'attendre à ce que leur communication nuise à l'application d'une loi du Canada ou d'une province ou à la tenue d'enquêtes licites. La Cour d'appel fédérale a rejeté l'argument du solliciteur général et a soutenu que l'alinéa 22(1)b) n'autorise pas le refus de communication du simple fait que celle-ci puisse comporter un effet dissuasif sur le processus d'enquête en général. La notion de préjudice énoncée à l'alinéa 22(1)b) ne dépasse pas le champ d'une enquête donnée, qu'elle soit en cours ou envisagée.

État de la situation

M. Ruby a demandé l'autorisation d'en appeler à la Cour suprême du Canada au sujet de la décision de la Cour d'appel fédérale concernant la constitutionnalité de l'article 51 de la *Loi sur la protection des renseignements personnels*. Le solliciteur général a demandé l'autorisation de présenter un appel incident de la décision de la Cour d'appel fédérale concernant l'interprétation de l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels*. La Cour suprême du Canada a accordé les autorisations d'appel et d'appel incident le 18 janvier 2001. J'ai demandé l'autorisation d'intervenir dans cette affaire relativement à l'alinéa 22(1)b). J'ai été autorisé à le faire le 25 mai 2001. Je déposerai mes arguments, qui diffèrent de ceux des deux parties, auprès de la Cour suprême du Canada.

Le Commissariat aux langues officielles (appelant) c. Robert Lavigne (intimé)

Cette affaire est actuellement en appel devant la Cour suprême du Canada. M. Lavigne s'est vu refuser l'accès à des renseignements personnels le concernant, qui se trouvaient dans les déclarations faites par les témoins lors d'une enquête menée par le Commissariat aux langues officielles. Le Commissariat a refusé l'accès en invoquant l'exemption prévue à l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels*.

M. Lavigne a présenté un recours en révision à la Section de première instance de la Cour fédérale concernant le refus du Commissariat aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*. Le Commissaire à la protection de la vie privée précédent et moi-même sommes intervenus à l'appui de M. Lavigne tout au long de cette affaire. Nos interventions ont porté fruit à la fois devant la Section de première instance de la Cour fédérale et la Cour d'appel fédérale.

Suivant une décision rendue à l'audience le 6 septembre 2000, la Cour d'appel fédérale a ordonné au Commissariat aux langues officielles de remettre à M. Lavigne ses renseignements personnels. La Cour d'appel fédérale s'est appuyée sur deux de ses décisions antérieures, *Rubin c. Canada (Ministre des Transports)* et *Ruby c. Canada (Solliciteur général)*, confirmant que l'exception prévue à l'alinéa 22(1)b) ne peut être invoquée que lorsqu'il y a preuve de préjudice dans le cadre d'une enquête donnée, l'exception ne peut être invoquée une fois que l'enquête est terminée, et il est interdit de refuser la communication des renseignements demandés sur la base que cette communication pourrait comporter un effet « dissuasif » sur des enquêtes futures possibles. La Cour

d'appel fédérale a rejeté l'argument du Commissariat aux langues officielles, à savoir qu'une interprétation différente était justifiée dans la présente affaire en raison du mandat conféré par la *Loi* au Commissaire aux langues officielles.

Les questions en litige qui étaient soulevées à la Cour suprême sont de savoir si la Cour d'appel a erré en concluant que les dispositions relatives à l'accès prévues à la *Loi sur la protection des renseignements personnels* l'emportent sur les dispositions relatives à la confidentialité de la *Loi sur les langues officielles* et de savoir si la décision de la Cour d'appel compromet gravement la capacité du Commissaire aux langues officielles d'appliquer la *Loi sur les langues officielles*.

État de la situation

Le Commissariat aux langues officielles a déposé une demande d'autorisation d'en appeler de la décision à la Cour suprême du Canada. L'autorisation d'appel a été accordée le 19 avril 2001. Le 21 août 2001, la Cour suprême du Canada m'a autorisé à intervenir au soutien de M. Lavigne. Mes soumissions en tant qu'intervenant seront déposés au début de décembre.



DEUXIÈME PARTIE

RAPPORT CONCERNANT LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

INTRODUCTION

L'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)*, représente une importante étape pour le Canada. Il s'agit d'un engagement clair du gouvernement afin de protéger notre droit fondamental à la vie privée, dans une ère où celle-ci est menacée comme elle ne l'a jamais été auparavant. Les percées technologiques qui révolutionnent notre mode de faire des affaires, conjugué à la détermination des entreprises de s'accaparer des renseignements personnels, les pays dans le monde entier reconnaissent l'importance de protéger la vie privée. En raison de la *LPRPDÉ*, Canada passe au rang des chefs de file mondiaux.

La partie 1 de la *Loi* énonce les conditions dans lesquelles les organismes peuvent recueillir, utiliser ou communiquer des renseignements personnels et accorde aux individus le droit d'accès aux renseignements personnels les concernant que détiennent les organismes ainsi que le droit de correction connexe. La *Loi* établit également le processus que peuvent emprunter les individus pour déposer une plainte officielle lorsqu'ils croient que leurs droits ont été violés ou lorsque les organisations n'ont pas respecté la *Loi*, ainsi que les recours judiciaires mis à leur disposition.

Cette partie de la *Loi* est mise en œuvre en trois étapes successives. Dans la première étape, qui a débuté le 1^{er} janvier 2001, la *Loi* vise les renseignements personnels, ceux sur la santé exceptés, qui sont recueillis, utilisés ou communiqués dans le cadre des activités commerciales ainsi que sur les employés d'entreprises fédérales. Celles-ci comprennent les banques, le secteur de la radiodiffusion, les

entreprises de transport interprovincial et les sociétés de téléphone.

La *Loi* porte également sur la communication des renseignements personnels qui sont échangés ou vendus à l'extérieur d'une province ou du pays. En outre, elle s'applique à tout le secteur commercial du Yukon, dans les Territoires du Nord-Ouest et le Nunavut, parce que toutes les entreprises locales y sont considérées comme des entreprises fédérales et sont ainsi du ressort du Parlement fédéral.

À compter du 1^{er} janvier 2002, la *Loi* s'appliquera également aux renseignements personnels sur la santé pour ce qui est des organismes et des activités visés lors de la première étape.

À compter du 1^{er} janvier 2004, toutes les dispositions de la partie 1 de la *Loi* auront force exécutoire partout au Canada dans le secteur privé réglementé au niveau provincial ou territorial, sauf lorsqu'une province ou un territoire a promulgué une loi que le gouverneur en conseil considère comme essentiellement similaire à la *Loi sur la protection des renseignements personnels et les documents électroniques*. En l'occurrence, la loi provinciale ou territoriale aura préséance pour toute collecte, utilisation ou communication de renseignements personnels par les entreprises qui sont visées par la loi provinciale ou territoriale. Cela signifie qu'à compter du 1^{er} janvier 2004, les droits à la vie privée des

Canadiens seront protégés dans tout le secteur privé, soit aux termes de la *Loi* fédérale ou d'une loi provinciale ou territoriale essentiellement similaire.

En tant que Commissaire à la vie privée du Canada, je suis chargé du contrôle d'application des règles régissant la collecte, l'utilisation et la communication des renseignements personnels établies dans la partie 1 de la *Loi*. Je reçois des plaintes et je mène des enquêtes et, comme il est prévu dans la *Loi sur la protection des renseignements personnels*, je joue le rôle d'ombudsman, tâchant de régler les différends par la négociation. Je peux également, suivant des motifs raisonnables, vérifier les pratiques de gestion des renseignements personnels d'une organisation.

Les pouvoirs en matière d'enquête qui sont conférés au Commissariat aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* correspondent à ceux prévus dans la *Loi sur la protection des renseignements personnels*, bien que je sois investi d'un mandat fort élargi en vue d'entreprendre des recherches sur les questions liées à la vie privée et de favoriser la sensibilisation des Canadiens à ces questions ainsi que leur compréhension.

Le présent rapport provisoire porte sur les activités associées à la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période du 1^{er} janvier 2001 au 30 novembre 2001.

MISE À JOUR DES LOIS PROVINCIALES ET TERRITORIALES

Détermination

d'« essentiellement similaire »

J'interpréterai une loi provinciale ou territoriale comme « essentiellement similaire » lorsqu'elle offre un degré et une qualité de protection de la vie privée égaux ou supérieurs à ceux de la *Loi fédérale*. La *Loi fédérale* constitue le seuil ou le niveau minimal. Une loi provinciale ou territoriale sur la protection des renseignements personnels doit assurer une protection au moins équivalente à celle de la loi fédérale, ou elle ne sera pas considérée comme essentiellement similaire.

Pour être considérée essentiellement similaire, une loi provinciale devra comprendre au bas mot les dix principes établis à l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Bien que les dix principes du code soient considérés comme interreliés et d'importance égale, j'aimerais m'attarder aux cinq éléments de la loi car ils constituent des composantes clés de la détermination de la nature essentiellement similaire d'une loi : le consentement, le critère de la personne raisonnable, les droits d'accès et de correction, la surveillance, et les voies de recours.

Consentement

Dans la mesure où la vie privée constitue le droit d'exercer un contrôle sur l'accès à sa personne et à ses renseignements personnels, il ne peut y avoir de contrôle sans consentement ni de vie privée sans contrôle.

L'exigence relative au consentement doit être le fondement de toute loi efficace sur la protection des renseignements personnels. La *Loi fédérale* précise que le consentement doit être éclairé, et que la collecte, l'utilisation et la communication des renseignements personnels sans le consentement de l'individu ne doivent se produire que dans des circonstances exceptionnelles déterminées.

Une organisation peut seulement recueillir, utiliser ou communiquer des renseignements personnels sur un individu dans la mesure où ce dernier a accordé son consentement (sauf dans des circonstances limitées établies dans la *Loi*).

Une fois recueillis, les renseignements personnels ne peuvent être utilisés ou communiqués qu'aux fins auxquelles le consentement a été accordé (sauf dans des circonstances limitées établies dans la *Loi*).

Critère de la personne raisonnable

Le critère de la personne raisonnable impose une autre contrainte importante aux organisations. La *Loi* prévoit que la collecte, l'utilisation et la communication de renseignements personnels doivent se faire seulement aux fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Entre autres, ce critère empêche les organisations d'énoncer en des termes trop larges ou vagues les fins auxquelles renseignements sont recueillis.

Droits d'accès et de correction

Les individus doivent avoir le droit d'accéder aux renseignements personnels que les organisations détiennent à leur sujet et corriger toute inexactitude (ou signaler tout désaccord au tiers qui a reçu les renseignements).

Surveillance

Lorsqu'un individu est d'avis que ses droits à la vie privée ont été violés ou que la *Loi sur la protection des renseignements personnels* n'a pas été respectée, l'individu doit pouvoir déposer une plainte à un organisme de surveillance pleinement autonome, qui est investi du mandat précis de régler les plaintes, de mener des enquêtes exhaustives, de soumettre à la médiation et à la conciliation, de formuler des recommandations ou de prendre des ordonnances. L'organisme de surveillance doit également être investi de pouvoirs d'enquête complets afin de saisir des documents, de

pénétrer dans des locaux, de contraindre à témoigner et de prendre l'initiative de vérifications des pratiques d'une organisation.

Voies de recours

À la suite de mon rapport sur une plainte auprès d'une organisation, la *Loi* fédérale permet au plaignant (ou à moi-même directement) de demander une audience à la Cour fédérale du Canada. Le plaignant ou moi-même pouvons demander à la Cour d'ordonner à l'organisation en question de rectifier ses pratiques de traitement des renseignements et de rendre publiques les mesures qu'elle a prises pour le faire. Il est possible de demander à la Cour d'accorder des dommages-intérêts au plaignant.

Il est possible d'en appeler des décisions de la Cour fédérale à la Cour d'appel fédérale ainsi qu'à la Cour suprême du Canada sur autorisation.

Je suis d'avis que toute loi provinciale qui est censée être « essentiellement similaire » doit comprendre des dispositions équivalentes en matière de recours.

Initiatives législatives en vue de réglementer le secteur privé

Jusqu'à présent, le Québec est la seule province au Canada qui a adopté des mesures de protection des renseignements personnels qui touchent les entreprises qui font affaire dans la province, tel qu'il est établi dans le Code civil. Ailleurs au Canada, deux gouvernements provinciaux – celui de la

Colombie-Britannique et de l'Ontario – ont commencé à explorer des options législatives afin de régler la collecte, l'utilisation et la communication des renseignements personnels dans le secteur privé. En effet, d'ici le 1^{er} janvier 2004, les gouvernements provinciaux devront avoir adopté une loi que le gouverneur en conseil estime, par décret d'exemption, essentiellement semblable à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Secteur de la santé

Les provinces de l'Alberta, du Manitoba et de la Saskatchewan ont adopté une loi sur la protection des renseignements personnels visant spécifiquement la santé. La *Loi* est actuellement en vigueur au Manitoba et en Alberta. En décembre 2000, l'Ontario a déposé son controversé projet de loi 159, *Loi sur la protection des renseignements personnels sur la santé*, qui est resté en plan au Feuilleton.

LOI POUR LE SECTEUR PUBLIC

La *Loi sur la protection des renseignements personnels* du Nouveau-Brunswick est entrée en vigueur en avril 2001. La *Loi sur l'accès à l'information et la protection de la vie privée* de l'Île-du-Prince-Édouard a reçu la sanction royale le 15 mai 2001, et entrera en vigueur en novembre 2002. Suivant la présentation et l'adoption de ces deux lois, toutes les provinces et tous les territoires au Canada, à l'exception de Terre-Neuve, offrent maintenant la protection réglementaire des renseignements

personnels que détiennent les ministères et les organismes fédéraux.

ENQUÊTES

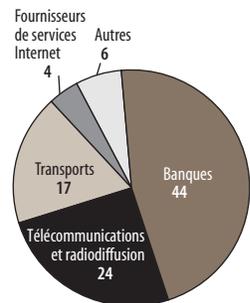
Au 30 novembre 2001, le Commissariat avait reçu 95 plaintes officielles aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Au cours de la première année depuis l'entrée en vigueur de la *Loi*, les plaintes ont essentiellement visé le secteur réglementé par le fédéral, dont près de la moitié se rapportaient aux banques.

Malgré la mise en œuvre progressive de la *Loi*, les organismes ont dû se préparer à son entrée en vigueur, et certains n'ont toujours pas intégré ses principes dans leurs pratiques d'affaires. De nombreuses plaintes ont soulevé des questions systémiques portant sur la violation des droits à la vie privée dans le secteur privé réglementé par le fédéral. Lorsqu'il était démontré que celles-ci étaient fondées, j'ai recommandé aux organisations qu'elles apportent d'importants changements aux politiques et procédures actuelles.

Aux termes de l'article 13 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, je suis autorisé à demander aux organisations de faire rapport sur les progrès réalisés pour mettre en œuvre ces changements, et suivant l'expérience jusqu'à date, il s'agit d'une démarche utile qui permettra d'assurer que les changements nécessaires sont apportés.

Nombre de plaintes selon le secteur

1^{er} janvier 2001 -
le 30 novembre 2001



La démarche que j'ai adoptée concernant les enquêtes et la résolution des plaintes ressemble à la démarche aux termes de la *Loi sur la protection des renseignements personnels*. Lorsqu'une plainte est déposée au Commissariat, j'avise officiellement l'organisation de la nature des allégations et je l'invite à présenter des observations. Dans la mesure du possible, j'essaie de régler les différends par la conciliation, la consultation, la persuasion et la médiation.

Je peux rendre l'une des conclusions suivantes dans le traitement d'une plainte :

- **Non fondée** : Aucun élément de preuve n'a été relevé qui me porte à conclure que l'organisation a violé la *Loi*.
- **Fondée** : L'enquête a permis d'établir que l'organisation n'a pas respecté une disposition de la *Loi*.
- **Résolue** : L'organisation a pris des mesures correctives pour remédier à la situation, ou le plaignant est satisfait des résultats de l'enquête du Commissariat.
- **Abandonnée** : Il s'agit d'enquêtes qui ont pris fin avant que toutes les allégations aient été pleinement examinées. Une affaire peut être abandonnée pour un nombre de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire.

LES CONCLUSIONS DU COMMISSAIRE

Voici mes conclusions aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* jusqu'au 30 novembre 2001. À des fins d'uniformité, les conclusions sont présentées dans le format tel qu'elles apparaîtront sur notre site Web à www.privcom.gc.ca . Depuis janvier 2001, le Commissariat a entrepris des enquêtes et rendu des conclusions ainsi que des recommandations d'enquêtes sur 27 plaintes aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*, et deux incidents. Les plaintes de nature presque identique ont été groupées et une seule conclusion a été rendue.

Activités de surveillance vidéo dans un endroit public [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Le Commissaire à l'information et à la vie privée des Territoires du Nord-Ouest et du Nunavut s'est plaint qu'une entreprise de services de sécurité ait indûment recueilli des renseignements personnels, sans le consentement des individus visés, en ayant recours à des caméras de surveillance installées dans la rue principale de Yellowknife.

Résumé de l'enquête

L'entreprise de services de sécurité en question avait installé, sur le toit de l'édifice de ses bureaux, quatre caméras vidéos braquées sur la principale intersection de Yellowknife, de même que deux moniteurs dans ses bureaux. Au début de mai 2001, le personnel de l'entreprise a surveillé pendant plusieurs jours des images en direct, jour et nuit. À plusieurs reprises, le personnel de l'entreprise a remarqué des délits et a communiqué avec le service de police. De l'aveu de l'entreprise, ses activités de surveillance faisaient partie d'un projet de marketing qui visait à stimuler les affaires. Vu la publicité négative que le projet a suscité, l'entreprise a retiré ses caméras moins d'une semaine après les avoir installées.

Conclusions du Commissaire (rendues le 15 juin 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que toute entreprise dans les Territoires du Nord-Ouest est une entreprise fédérale au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3 de l'annexe I précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Le Commissaire a conclu que puisque la surveillance des faits et gestes du public constituait le principal objectif de l'installation de l'équipement de surveillance vidéo, les renseignements en cause étaient considérés comme personnels aux termes de la *Loi*. L'entreprise ayant admis que ses activités de surveillance vidéo relevaient d'un projet de marketing, le Commissaire a conclu qu'il s'agissait d'une activité commerciale au sens de la *Loi*.

Le fait que l'image vidéo était transmise en direct et n'était pas enregistrée a été jugé non pertinent puisqu'au regard de la *Loi*, les renseignements personnels ne se limitent pas aux seuls renseignements enregistrés. En se fondant sur les preuves, le Commissaire était d'avis que les individus n'avaient pas consenti à la collecte. Il a conclu que l'entreprise avait recueilli des renseignements personnels sans le consentement des intéressés au mépris du principe énoncé à l'article 4.3.

Au moment de présenter ses conclusions, le Commissaire a formulé les commentaires suivants : [TRADUCTION] « Il peut arriver qu'il soit approprié de surveiller des endroits publics pour des raisons de sécurité publique. Il faut toutefois limiter cette pratique aux seuls cas où il est possible d'en démontrer le besoin. Il faut que seules les autorités publiques légitimes puissent effectuer ces activités, et seulement d'une façon qui tienn compte toutes les mesures de protection de

la vie privée prévues dans la *Loi*. Dans notre société, la surveillance non autorisée des endroits publics, à des fins commerciales, par des organisations du secteur privé n'a pas sa place. »

Le Commissaire a donc conclu que la plainte était fondée.

AUTRES CONSIDÉRATIONS

Il n'était pas nécessaire de prendre d'autres mesures à l'égard de la plainte, puisque l'entreprise avait déjà retiré les caméras avant que le Commissaire ait rendu ses conclusions. Néanmoins, l'affaire n'était pas tout à fait réglée, du fait que l'entreprise de services de sécurité avait signalé qu'elle avait l'intention de continuer de déployer des efforts dans le but d'offrir des services de surveillance vidéo aux membres de la communauté de Yellowknife. Le Commissaire a indiqué à l'entreprise que son projet de surveillance vidéo du public à des fins commerciales est illégal et qu'elle devait l'abandonner.

Messages électroniques non sollicités d'un fournisseur de services Internet [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Une cliente s'est plainte que son fournisseur de services Internet (FSI), en lui envoyant des communications électroniques non sollicitées, ait utilisé sans son consentement des renseignements personnels la concernant, à savoir son adresse électronique.

Résumé de l'enquête

Le FSI de la plaignante lui avait fait parvenir plusieurs messages électroniques non sollicités portant sur ses services. Tout d'abord, elle s'est plainte directement auprès du FSI, mais la suggestion de l'entreprise, qui l'a invitée tout simplement à reconfigurer son fureteur de façon que les messages soient envoyés directement dans un sous-répertoire de courrier en vrac ou dans la corbeille, ne l'a pas satisfaite. Elle soutenait que l'utilisateur ne devrait pas porter le fardeau de déceler les communications électroniques non sollicitées du FSI. Pour sa part, l'entreprise soutenait qu'elle était en droit d'envoyer de tels messages, en vertu des modalités et conditions de l'entente d'abonnement, qui comprend une clause de consentement.

La plaignante, dont le premier abonnement d'un an était un cadeau d'un ami, n'avait pas étudié personnellement ces modalités et conditions au départ, mais en a pris connaissance par la suite, au renouvellement de son abonnement après la première année. La plaignante a renouvelé son abonnement auprès de la même entreprise même si à ce moment-là, sa plainte n'était toujours pas réglée.

*Conclusions du Commissaire
(rendues le 3 juillet 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les fournisseurs de services Internet sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3 de l'annexe I précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Après avoir examiné l'entente d'abonnement du FSI en question, le Commissaire était d'avis que la pratique d'envoi de communications électroniques périodiques à la clientèle était décrite clairement dans l'entente. Par conséquent, il a jugé qu'il était raisonnable que les clients s'attendent à recevoir, de temps à autre, de pareilles communications. De plus, il a considéré que la plaignante avait consenti à cette pratique en renouvelant son abonnement. Il a conclu que dans cette affaire, le FSI n'avait pas contrevenu au principe énoncé à l'article 4.3.

Le Commissaire a donc conclu que la plainte n'était pas fondée.

AUTRES CONSIDÉRATIONS

Le Commissaire a signalé à la plaignante qu'il estimait que la première suggestion formulée

par le FSI en vue de résoudre son problème était raisonnable.

Il a en outre formulé le commentaire suivant : [TRADUCTION] « Les communications électroniques sont conformes avec l'objet du consentement d'utilisation de l'adresse électronique qui, à l'origine, avait été obtenu pour permettre la prestation efficace des services du FSI. »

Le Commissaire étudie le domaine de compétence dans une affaire de communication de renseignements d'une filiale bancaire à un tiers [article 30]

Plainte

Un client s'est plaint qu'une société de placement, filiale d'une banque à charte, ait indûment communiqué à un tiers, c'est-à-dire à l'organisme de réglementation qui surveille les activités de la société, des renseignements personnels relatifs à ses opérations financières.

Résumé de l'enquête

Dans cette affaire, le Commissaire devait déterminer si la plainte relevait ou non de ses compétences.

*Conclusions du Commissaire
(rendues le 19 juillet 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique strictement aux entreprises fédérales et aux communications de renseignements personnels pour contrepartie à l'extérieur

d'une province. Les banques sont des entreprises fédérales au sens de la *Loi*. Toutefois, dans la présente affaire, encore que la société de placement soit une filiale bancaire, elle est exploitée en tant que personne morale, elle ne communique pas de renseignements pour contrepartie à l'extérieur de la province, et elle est sous réglementation provinciale. À l'heure actuelle, la société en question n'est pas visée par la *Loi*.

Le Commissaire a conclu qu'il n'était pas de son ressort de faire enquête sur cette plainte.

Une cliente d'une banque demande des renseignements sur sa cote de crédit [principe énoncé à l'article 4.9 de l'annexe 1, et article 8]

Plainte

Une cliente s'est plainte qu'une banque ne lui ait pas permis de consulter ses renseignements personnels concernant sa cote de crédit.

Résumé de l'enquête

La plaignante avait téléphoné à la succursale de la banque en question pour demander des renseignements au sujet de sa cote de crédit. Un représentant du service à la clientèle de la succursale lui a répondu que la banque ne divulguait pas ces renseignements à ses clients. La banque, ayant appris le dépôt de cette plainte, a entrepris une recherche approfondie dans ses dossiers et a signalé par la suite qu'il ne s'y trouvait pas d'entente ou de demande de crédit au nom de la plaignante, et que par conséquent, la banque ne disposait pas de

cote de crédit pour cette cliente. La plaignante a confirmé subséquemment qu'elle n'avait pas conclu d'entente de crédit avec cette banque, à laquelle elle n'avait par ailleurs jamais présenté de demande de crédit.

Conclusions du Commissaire (rendues le 23 juillet 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les établissements financiers sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.9 de l'annexe 1 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation qui en est faite et de leur communication à des tiers, et lui permettre de les consulter. L'article 8 établit les conditions en fonction desquelles une organisation serait réputée avoir refusé d'acquiescer à la demande.

Le Commissaire était convaincu que les dossiers de la banque ne contenaient pas les renseignements que la plaignante avait demandés. Il a donc conclu que la banque n'avait pas privé la plaignante de son droit de consulter les renseignements personnels qui la concernent en vertu de l'article 8 de la *Loi*.

Le Commissaire a conclu que la plainte n'était pas fondée.

**Conservation de renseignements personnels
après le rejet d'une demande
[principe énoncé à l'article 4.5 de l'annexe 1]**

Plainte

Une particulière qui avait présenté une demande de carte de crédit s'est plainte que la banque, après l'avoir rejetée, ait refusé de satisfaire à sa requête pour que les renseignements personnels recueillis dans sa demande soient supprimés des dossiers de la banque.

Résumé de l'enquête

La plaignante avait présenté en personne une demande de carte de crédit, mais la banque en question l'avait rejetée. La plaignante a ensuite demandé que les renseignements personnels qu'elle avait inscrits dans sa demande soient retirés du système informatique de la banque. Le directeur de la succursale a répondu que le pouvoir de supprimer des renseignements ne lui avait pas été délégué, et il n'a pas tenté d'établir s'il était possible d'entreprendre d'autres démarches à cette fin.

De fait, l'agent de protection de la vie privée et le gestionnaire des opérations des cartes de crédit étaient investis par délégation du pouvoir de retirer ces renseignements sur demande spéciale, mais dans la présente affaire, la demande de la plaignante n'a pas été transmise à l'un ou l'autre de ces responsables. À la banque, la pratique courante relative aux demandes de carte de crédit présentées en personne consistait à saisir immédiatement

les renseignements personnels dans le système informatique de la succursale, puis de les envoyer au système hôte du centre d'évaluation des dossiers de financement pour soumettre la demande à la décision de la banque. Si la demande était refusée, les renseignements n'étaient pas éliminés automatiquement. Sauf sur demande spéciale de l'individu dont la demande avait été rejetée, les renseignements personnels le concernant étaient conservés dans le système informatique de la banque, où le personnel de la succursale pouvait y avoir accès indéfiniment.

**Conclusions du Commissaire
(rendues le 23 juillet 2001)**

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.5 de l'annexe 1 stipule que les renseignements personnels doivent être conservés aussi longtemps que nécessaire pour la réalisation des fins auxquelles ils ont été recueillis.

Le Commissaire a jugé déraisonnable le fait que si la plaignante n'avait pas insisté pour qu'ils soient retirés, les renseignements personnels la concernant auraient pu demeurer

accessibles indéfiniment à la succursale, après que la banque les a utilisés pour des fins auxquelles ils avaient été recueillis (c.-à-d. la prise de décision au sujet de la carte de crédit). Il a conclu que dans cette affaire, la banque avait contrevenu au principe énoncé à l'article 4.5.

Néanmoins, le Commissaire a également fait observer que la banque avait, par la suite, supprimé les renseignements personnels concernant la plaignante et confirmé qu'ils n'avaient pas été communiqués à un tiers. En outre, il a signalé que le plaignant était satisfaite de ce règlement.

Le Commissaire a donc conclu que la plainte était fondée et résolue.

AUTRES CONSIDÉRATIONS

En vue d'aborder les irrégularités décelées dans l'enquête du Commissaire, la banque en question a convenu d'entreprendre un examen approfondi de ses pratiques courantes de conservation des renseignements personnels. La banque a également convenu de mettre en œuvre une stratégie de communication visant à informer les employés et les clients de sa procédure relative aux plaintes concernant la protection des renseignements personnels.

Sûreté du service téléphonique automatisé d'une banque [principe énoncé à l'article 4.7 de l'annexe 1]

Plainte

Invoquant plusieurs dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques*, un individu s'est plaint qu'une banque n'ait pas appliqué les mesures de sécurité convenables pour protéger les renseignements concernant la clientèle qui sont communiqués au moyen de son service téléphonique automatisé.

Résumé de l'enquête

La banque en question offre un service téléphonique automatisé aux titulaires de cartes Visa qui ne font pas d'autres opérations auprès de cette banque. Les utilisateurs de ce service ne peuvent faire de transactions mais peuvent consulter certains renseignements relatifs à leur compte Visa en composant les 16 chiffres de leur numéro de compte et, suivant le choix au hasard du système, les quatre derniers chiffres du numéro de téléphone à domicile ou l'année de naissance du titulaire de la carte.

Conclusions du Commissaire (rendues le 23 juillet 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette

plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.7 de l'annexe 1 précise que les renseignements personnels doivent être protégés par une organisation au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Après avoir examiné la plainte, le Commissaire a jugé la préoccupation du plaignant valable. Il a établi qu'un processus de codage reposant à un point tel sur le numéro de téléphone ou l'année de naissance du titulaire de la carte ne suffisait pas à empêcher des personnes non autorisées de consulter des renseignements personnels à caractère délicat concernant les utilisateurs. Il a jugé que la banque n'était pas en conformité avec le principe énoncé à l'article 4.7.

Néanmoins, le Commissaire a observé que la banque avait proposé et entrepris un plan d'action détaillé en trois étapes visant à régler les problèmes de sécurité soulevés dans la plainte. En outre, il a observé que le plaignant et lui-même ont jugé tous les aspects du plan satisfaisants.

Le Commissaire a donc conclu que la plainte était fondée et résolue.

AUTRES CONSIDÉRATIONS

Le plan d'action proposé par la banque comprend les trois étapes suivantes :

Immédiat : L'accès automatisé au compte Visa du plaignant est bloqué, de sorte que toute tentative non autorisée de consultation des renseignements personnels du plaignant échouera. Le plaignant pourra lui-même consulter son compte par l'intermédiaire d'un mandataire, au moyen d'un mot de passe préétabli.

À court terme : D'ici le 31 octobre 2001, les clients de Visa qui ne font pas d'autres opérations auprès de cette banque pourront bloquer l'accès téléphonique automatisé à leur compte sur demande et pourront, s'ils le souhaitent, transiger directement avec un mandataire. Cette étape comprend une stratégie de communication visant à informer les clients à ce sujet.

À long terme : La banque a convenu de mettre en œuvre, au cours des trois prochaines années, un nouveau service bancaire téléphonique qui remédiera aux préoccupations des clients quant à la protection de la vie privée et à la sûreté du service, et de rendre compte des progrès accomplis au Commissaire à la protection de la vie privée au plus tard le 31 juillet 2002.

Le Commissaire a formulé le commentaire suivant : [TRADUCTION] « Je suis d'avis que les mesures que [la banque] a prises pour résoudre les problèmes de sûreté soulevés ... sont acceptables. »

Un musicien s'oppose à ce qu'une organisation professionnelle recueille des renseignements sur son salaire [article 2]

Plainte

Un musicien s'est plaint que l'organisation professionnelle chargée de représenter ses intérêts ait, sans son consentement, recueilli des renseignements personnels à son sujet, à savoir son salaire annuel, auprès de son employeur.

Résumé de l'enquête

Le plaignant est le seul musicien à l'emploi d'un certain établissement. L'organisation professionnelle en question doit, au nombre de ses activités, recueillir les droits d'auteur pour ses membres, conformément aux exigences de la *Loi sur le droit d'auteur*. En vue de produire le tarif applicable auprès de la Commission du droit d'auteur et de percevoir les redevances, l'organisation doit déterminer avant tout le budget global de divertissement d'un établissement donné. La préoccupation du plaignant venait du fait que puisqu'il était le seul musicien à l'emploi de l'établissement en question, un tiers aurait pu le reconnaître comme seul bénéficiaire de l'affectation réservée aux salaires dans le budget de divertissement. Toutefois, l'identification des musiciens ou la détermination du nombre de musiciens travaillant dans un établissement ne présentent pas d'intérêt pour l'organisation dans la collecte de tels renseignements, et c'est pourquoi elle ne recueille pas de noms ou de

nombres. En outre, l'organisation ne publie pas et ne communique pas à des tiers les renseignements qu'elle recueille au sujet de l'établissement.

Conclusions du Commissaire (rendues le 23 juillet 2001)

COMPÉTENCE : L'organisation professionnelle en question a affirmé qu'elle était visée par la *Loi sur la protection des renseignements personnels et les documents électroniques*. Le Commissaire n'a pas contesté cette position.

APPLICATION : Selon l'article 2 de la *Loi*, un renseignement personnel se dit de « [...] tout renseignement concernant un individu identifiable [...] ».

En se fondant sur les preuves, le Commissaire était d'avis que l'organisation professionnelle était autorisée par la *Loi* à recueillir les renseignements en cause et que la collecte ne portait pas sur des renseignements personnels concernant un individu identifiable. Par conséquent, il a conclu que la collecte n'était donc pas visée par les dispositions de la *Loi*.

Le Commissaire a conclu que la plainte n'était pas fondée.

AUTRES CONSIDÉRATIONS

Au moment de communiquer ses conclusions, le Commissaire a formulé le commentaire suivant : [TRADUCTION] « Puisque j'ai établi que les renseignements recueillis ne sont pas personnels, j'ai jugé que je n'ai pas besoin de poser de conclusions quant à leur

bien-fondé en considération des articles 4.3 (consentement) et 4.4 (limitation de la collecte) de l'annexe 1 et de l'article 7 (collecte à l'insu de l'intéressé et sans son consentement) de la *Loi*, qui, autrement, auraient pu s'appliquer à la présente plainte. »

Utilisation et communication de renseignements personnels dans les annuaires téléphoniques [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Invoquant plusieurs dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques*, un particulier s'est plaint qu'une entreprise de télécommunications :

1. ait utilisé et communiqué des renseignements personnels concernant les clients à leur insu et sans avoir obtenu leur consentement, en publiant leur nom, leur adresse et leurs numéros de téléphone dans les pages blanches de l'entreprise et sur deux sites Web; et
2. ait indûment exigé des clients qu'ils paient pour ne pas publier les renseignements personnels qui les concernent.

Résumé de l'enquête

L'entreprise de télécommunications en question publie les nom, adresse et numéros de téléphone de ses clients dans ses pages blanches et sur son propre site Web d'assistance-annuaire. Conformément aux règlements du CRTC, l'entreprise transmet ces

renseignements à la filiale de Bell Canada qui exploite du site Web « Canada 411 ». Les clients sont invités à préciser la façon dont ils souhaitent que les renseignements personnels les concernant figurent dans les pages blanches de l'entreprise et peuvent demander que ces renseignements ne soient pas publiés. L'entreprise exige des frais de service aux clients qui demandent la non-publication, conformément aux règlements du CRTC. En outre, l'entreprise, moyennant frais, fournit à certaines organisations des services de listes qui ne comprennent pas de renseignements sur les clients qui ont choisi la non-publication et sur les clients qui demandent que leur nom soit rayé.

Conclusions du Commissaire (rendues le 14 août 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont tenues pour des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Au sujet du consentement, le Commissaire a jugé que la question que l'entreprise posait à ses clients quant à la façon dont les renseignements les concernant devraient figurer dans les pages blanches était pertinente. Il a établi que la question implique en soi la publication éventuelle des renseignements dans des annuaires auxquels le public a accès. Les clients qui choisissent de ne pas se prévaloir de l'option de non-publication consentent implicitement à ce que des renseignements personnels les concernant deviennent accessibles au public. De plus, puisque les renseignements publiés par la suite sur d'autres supports correspondent tout à fait à ceux qui sont publiés dans les pages blanches, pour l'application des règlements en vertu de la *Loi*, ils sont également tenus pour des renseignements auxquels le public a accès et il est possible de les recueillir, de les utiliser et de les communiquer sans le consentement de la personne concernée. En somme, le Commissaire a conclu que l'entreprise avait obtenu un consentement valable et observait les règlements sur les renseignements auxquels le public a accès.

Au sujet des frais exigés pour la non-publication des renseignements concernant les clients, le Commissaire a constaté que l'entreprise avait dûment demandé la permission du CRTC, qui la lui avait accordée, en vertu de l'Ordonnance Télécom 98-109, qui stipule que les sociétés de télécommunications peuvent exiger jusqu'à

au plus 2 \$ par mois pour un service de numéro non publié. Par conséquent, il a conclu que l'entreprise en cause était habilitée à exiger son tarif mensuel de non-publication établi à 2 \$.

Le Commissaire a conclu que la plainte n'était pas fondée.

Inscription du numéro de compte sur un chèque à la banque [paragraphe 5(3)]

Plainte

Un individu s'est plaint qu'une banque ait créé un risque de communication inappropriée à un tiers de renseignements personnels le concernant, sans son consentement, lorsqu'un caissier a inscrit son numéro de compte à l'endos d'un chèque au moment de l'encaissement.

Résumé de l'enquête

Le plaignant avait visité une succursale de sa banque pour encaisser un chèque personnel d'un tiers. Le caissier a inscrit le numéro de compte du plaignant à l'endos du chèque. La préoccupation du plaignant tenait au fait que s'il fallait retourner le chèque au tiré pour quelque raison que ce soit, son numéro de compte serait divulgué à cette personne.

La banque a fait valoir que lorsqu'elle encaisse des chèques, elle accorde un crédit jusqu'à ce que la valeur du chèque puisse être portée au débit du compte du tiré. Dans des cas

exceptionnels (p. ex. fraude ou insuffisance de provision), la banque doit pouvoir recourir à un moyen efficace pour récupérer la somme du chèque auprès du client qui l'a encaissé. À cette fin, les noms inscrits au verso des chèques ne constituent pas un moyen suffisamment efficace, car ils peuvent différer pour la peine des noms exacts sous lesquels les comptes bancaires des clients sont ouverts. La banque a soutenu que l'inscription des numéros de compte sur les chèques est une pratique de longue date dans toute l'industrie, et qu'il faut l'appliquer pour protéger les intérêts de la banque en veillant à ce qu'elle puisse percevoir les sommes auprès du tiré ou les récupérer auprès de la personne qui dépose ou encaisse le chèque.

*Conclusions du Commissaire
(rendues le 14 août 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le paragraphe 5(3) prévoit que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Le Commissaire a établi que la pratique bancaire qui consiste à inscrire le numéro de compte sur le chèque au moment de l'encaissement est raisonnable et qu'il est raisonnable qu'un client s'attende à ce qu'il en soit ainsi. Le Commissaire était d'avis que le plaignant avait donc consenti implicitement à la collecte, à l'utilisation et à la communication de renseignements personnels qui le concernent. Le Commissaire a conclu qu'il n'avait pas été établi que cette pratique contrevenait à la *Loi*.

Il a donc conclu que la plainte n'était pas fondée.

AUTRES CONSIDÉRATIONS

Au moment de présenter ses conclusions, le Commissaire a formulé le commentaire suivant : [TRADUCTION] « Lorsqu'il remet un chèque pour l'encaisser, le client de la banque donne son consentement implicite à la communication des renseignements personnels qui figurent à l'endos du chèque, au même titre que le tiré donne son consentement explicite à la communication des renseignements personnels le concernant (qui figurent au verso du chèque) au tireur. »

Une entreprise de camionnage recueille des renseignements personnels prévus pour Douanes Canada [principe énoncé à l'article 4.4 de l'annexe 1]

Plainte

Un employé licencié s'est plaint que son ancien employeur, entreprise internationale de camionnage, ait indûment tenté de recueillir des renseignements personnels à son sujet car elle a insisté pour qu'il remplisse et lui renvoie une formule de demande pour un programme établi par l'Agence des douanes et du revenu du Canada (ADRC).

Résumé de l'enquête

L'entreprise de camionnage en question avait envoyé au plaignant, l'un de ses conducteurs internationaux, une lettre indiquant qu'il devait remplir une « demande de participation au programme d'inscription des chauffeurs du secteur commercial » dans le cadre du nouveau Programme d'autocotisation des douanes établi par l'ADRC. La lettre indiquait également que le conducteur devait renvoyer la demande remplie à l'entreprise. Le plaignant a refusé, souhaitant éviter que son employeur ne puisse consulter les renseignements personnels qu'il devait inscrire sur la formule. L'entreprise lui a fait parvenir une seconde lettre qui l'ordonnait au plaignant de remplir et de renvoyer la demande avant une certaine date, sans quoi il ferait l'objet de mesures

disciplinaires en vertu de l'entente collective, et son emploi serait compromis. De nouveau, le plaignant n'a pas accédé à cette demande, et l'entreprise a mis fin à son emploi cinq jours après la date indiquée. Aux dires de l'entreprise, l'ADRC attendait des employeurs qu'ils recueillent les demandes et les remettent à l'ADRC pour le compte des conducteurs. De fait, l'ADRC indique clairement, tant sur la formule de demande que dans la brochure portant sur le programme, que les conducteurs doivent remettre leur demande remplie directement au centre de traitement de l'ADRC, à Niagara Falls.

Conclusions du Commissaire (rendues le 17 août 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises interprovinciales de camionnage sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.4 de l'annexe 1 stipule que l'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et qu'elle doit le faire de façon honnête et licite.

Le Commissaire a établi que, bien que les conducteurs remplissent une demande pour le Programme d'autocotisation des douanes et la renvoyer à l'ADRC, il n'était pas nécessaire ou approprié que l'entreprise recueille elle-même les renseignements. De plus, il a établi qu'il n'était pas honnête de menacer les employés de les relever de leurs fonctions dans le but de recueillir les renseignements. Il a jugé que l'entreprise n'était pas conforme au principe énoncé à l'article 4.4.

Le Commissaire a observé que l'entreprise avait modifié rapidement sa politique afin que les conducteurs ne soient plus tenus de renvoyer leur demande à l'entreprise. Il n'estimait toutefois pas que la plainte était réglée car que l'employé devait réintégrer dans l'entreprise et qu'il obtienne réparation. Le Commissaire a signalé qu'il avait l'intention de donner suite à cette plainte auprès de l'entreprise.

Le Commissaire a conclu que la plainte était fondée.

AUTRES CONSIDÉRATIONS

Le plaignant a subséquemment informé le Commissaire qu'un règlement au sujet de son congédiement était intervenu par arbitrage et que pour ce motif, il estimait que la plainte avait été réglée de façon satisfaisante.

Une banque perd des renseignements personnels concernant une cliente [principe énoncé à l'article 4.7 de l'annexe 1, et paragraphe 12(2)]

Plainte

Une cliente s'est plainte qu'une banque ait manqué de protéger des renseignements personnels la concernant lorsque des documents contenant ses numéro d'assurance sociale (NAS), nom, adresse et numéro de téléphone non inscrit à l'annuaire ont été perdus au cours d'un transfert d'un bureau à l'autre.

Résumé de l'enquête

Développement des ressources humaines
Canada avait remis un nouveau numéro d'assurance sociale à la plaignante après qu'elle eut découvert que le précédent avait été utilisé frauduleusement. Plus tard, elle a rempli des formules dont la banque avait besoin pour modifier avec son nouveau NAS des renseignements concernant son compte de placement. Elle a remis les formules remplies au personnel d'une succursale locale de la banque afin qu'elles soient transmises au bureau de la succursale où le compte de placement est administré. Les documents ont été perdus au cours du transfert.

*Conclusions du Commissaire
(rendues le 7 septembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.7 de l'annexe 1 précise que les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Le paragraphe 12(2) stipule que le Commissaire peut tenter de parvenir au règlement de la plainte en ayant recours à un mode de règlement des différends, notamment la médiation et la conciliation.

Dans l'enquête du Commissaire, les parties se sont montrées intéressées dès le départ à régler la plainte. Il s'en est suivi une discussion jusqu'à ce qu'intervienne, en fin de compte, un règlement à la satisfaction des deux parties. De plus, le Commissaire était d'avis que la banque en question avait pris des mesures afin de s'assurer que les politiques, pratiques et procédures appropriées de protection étaient en place.

Le Commissaire a donc conclu que la plainte était réglée et qu'il n'était pas nécessaire de prendre d'autres mesures.

AUTRES CONSIDÉRATIONS

La plaignante et la banque se sont estimées satisfaites du rôle joué par le Commissariat dans le règlement de cette plainte.

Un demandeur de carte de crédit s'oppose à la politique sur l'échange de renseignements d'une banque

Plainte

Un individu s'est plaint qu'une banque ait refusé de traiter sa demande de carte de crédit parce qu'il ne voulait pas consentir à la politique sur l'échange de renseignements de la banque.

Résumé de l'enquête

En remplissant une demande de carte de crédit, le plaignant en a modifié à la main les modalités et conditions. Il espérait exprimer de la sorte son désaccord quant à la politique sur l'échange de renseignements personnels de la banque et exercer son droit de refuser que des renseignements personnels qui le concernent soient communiqués et de refuser de recevoir les services de marketing direct de la banque. La banque lui a envoyé par la suite une lettre qui indiquait qu'il lui était impossible de traiter sa demande telle quelle parce que le libellé avait été modifié. Le plaignant a compris que la lettre indiquait que la banque refusait de lui accorder une carte de crédit à moins qu'il ne consente à sa politique sur l'échange de renseignements. Dans une deuxième lettre, la banque a indiqué au

plaignant que les demandeurs étaient en droit de choisir de ne pas recevoir les services de marketing direct, et que sa propre demande lui avait été renvoyée tout simplement parce qu'il l'avait modifiée. De plus, la banque a offert au plaignant d'examiner de nouveau sa demande de carte de crédit et, du même coup, de rayer son nom des listes de marketing direct et de marketing croisé. Le plaignant a accepté cette offre.

Le plaignant, qui s'est finalement vu accorder une carte de crédit, s'est déclaré satisfait du suivi de la banque et a indiqué que son dossier de plainte auprès du Commissariat à la protection de la vie privée pouvait être fermé.

Par conséquent, cette plainte a été abandonnée.

Une banque accusée de retenir des certificats d'obligation [principe énoncé à l'article 4.9 de l'annexe 1, et article 8]

Plainte

Une particulière s'est plainte qu'une banque ait refusé qu'elle consulte des renseignements personnels la concernant, à savoir deux « obligations pour la petite entreprise », immatriculées à son nom, qu'elle croyait que la banque détenait.

Résumé de l'enquête

La plaignante a précisé que les documents qu'elle demandait étaient deux « obligations pour la petite entreprise » sur support papier

ou sous forme de certificats. En 1982, la plaignante et son conjoint avaient consolidé leurs dettes existantes à la banque en question dans le cadre du Programme des obligations des petites entreprises, initiative fédérale qui accordait une exemption d'intérêts aux emprunteurs. Dès 1984, la banque avait signalé à la plaignante que « l'obligation pour la petite entreprise » n'était qu'une expression et que le seul véritable document dûment signé ayant trait au Programme des obligations des petites entreprises était la formule intitulée « Choix commun à l'égard d'une obligation pour le développement de la petite entreprise ». La banque et Industrie Canada ont confirmé que cette formule était le seul document directement relié au programme. Il n'y avait jamais eu d'obligations pour la petite entreprise sur support papier ou sous forme de certificats. En 1998, au cours d'une poursuite relative à la défaillance de la plaignante à l'égard de son contrat de prêt, la banque avait dû remettre à la plaignante et à son avocat tous les documents relatifs à sa participation au Programme des obligations des petites entreprises qu'elle détenait. La plaignante avait alors reçu sa formule dûment signée de « Choix commun à l'égard d'une obligation pour le développement de la petite entreprise », qu'elle avait toujours en sa possession lorsqu'elle a déposé sa plainte auprès du Commissariat à la protection de la vie privée.

*Conclusions du Commissaire
(rendues le 18 septembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.9 de l'annexe 1 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation de leur communication à des tiers, et lui permettre de les consulter. L'article 8 établit les conditions en fonction desquelles une organisation serait réputée avoir refusé d'acquiescer à la demande.

Le Commissaire n'a relevé aucun élément de preuve démontrant l'existence de documents concernant les obligations pour la petite entreprise, hormis celui que la plaignante avait déjà reçu. Convaincu que les documents que demandait la plaignante n'existaient pas, le Commissaire a conclu que la banque n'avait pas privé la plaignante de son droit de les consulter.

Le Commissaire a donc conclu que la plainte n'était pas fondée.

Vente de renseignements sur les habitudes de prescription des médecins [articles 2 et 3]

Deux Plaintes

Dans deux plaintes distinctes un individu et un médecin se sont plaints qu'une branche canadienne d'une entreprise internationale de marketing des États-Unis ait indûment communiqué des renseignements personnels en recueillant et en vendant des données relatives aux habitudes de prescription des médecins sans leur consentement.

Résumé de l'enquête

L'entreprise de marketing en question recueille, auprès de pharmacies et d'autres sources canadiennes, des données relatives aux ordonnances médicales. Les renseignements réunis comprennent des noms, des numéros d'identité, des numéros de téléphone et des particularités de prescription des médecins. Ces renseignements sont transmis au centre de traitement des données de l'entreprise aux États-Unis, où l'entreprise produit des produits d'information personnalisés. Ces produits, en général, dressent une liste des médecins d'un certain territoire et les classent, individuellement ou en groupes, suivant leur activité mensuelle de prescription de divers types ou diverses catégories de médicaments. Ces produits d'information sont ensuite transférés à l'établissement de Montréal, où ils sont communiqués aux clients, moyennant

frais. Les représentants en produits pharmaceutiques de plusieurs provinces canadiennes achètent régulièrement ces produits.

*Conclusions du Commissaire
(rendues le 21 septembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique à toute communication de renseignements personnels pour contrepartie à l'extérieur d'une province. Puisque les renseignements en cause étaient régulièrement communiqués à l'extérieur de la province, le Commissaire a établi qu'il s'agissait de communications de renseignements pour contrepartie à l'extérieur d'une province et par conséquent, il était tenu de recevoir cette plainte et de faire enquête.

APPLICATION : Selon l'article 2 de la *Loi*, un renseignement personnel se dit de « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail ». L'article 3 de la *Loi* expose l'objet de la *Loi*, qui consiste à établir un équilibre entre le droit des individus à la vie privée et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables.

Le Commissaire devait déterminer avant tout si les renseignements en cause étaient des renseignements personnels au sens et selon la portée et l'objet de la *Loi*. Dans cette question, le sens de « renseignement personnel », bien que vaste, ne l'est pas assez pour englober tous les renseignements associés à un individu, de l'avis du Commissaire. L'ordonnance individuelle, quoiqu'elle puisse révéler des renseignements au sujet du patient, n'est pas, de façon significative, un renseignement concernant le médecin prescripteur comme individu. Il s'agit plutôt d'un renseignement concernant le processus professionnel qui a débouché sur sa délivrance, et il faudrait considérer que l'ordonnance est un produit de travail, c'est-à-dire le résultat tangible de l'activité professionnelle du médecin.

Le Commissaire a établi qu'une interprétation de « renseignement personnel » qui serait assez vaste pour englober les ordonnances ou les habitudes de prescription ne permettrait pas de réaliser l'objet exposé à l'article 3 de la *Loi* (voir ci-dessus). Plus précisément, il ne serait pas raisonnable d'élargir la définition pour englober les ordonnances, de crainte qu'elle ne s'applique en outre à tous les autres produits de travail, comme les avis juridiques ou les documents rédigés dans le cadre du travail. Il apparaît qu'il n'est pas plus raisonnable d'élargir la définition pour englober les habitudes de prescription, de crainte qu'elle

ne s'applique en outre aux habitudes que permettraient de découvrir d'autres genres de produits de travail, et par conséquent, que de nombreux genres de rapports commerciaux légitimes pour les consommateurs ne soient interdits.

En somme, le Commissaire a conclu que les renseignements sur les ordonnances, que ce soit sous forme d'ordonnances individuelles ou sous forme de tendances dégagées d'un certain nombre d'ordonnances, ne sont pas des renseignements personnels concernant un médecin.

Le Commissaire a donc conclu que les plaintes n'étaient pas fondées.

AUTRES CONSIDÉRATIONS

En raison de l'intérêt général que cette plainte a suscité auprès du public, le Commissaire a publié sa lettre de conclusions sous forme de communiqué, le 2 octobre 2001.

Obstacles à la démarche d'un exécuteur testamentaire tâchant d'obtenir des renseignements concernant un coffre bancaire [principes énoncés aux articles 4.5 et 4.9 de l'annexe 1, et paragraphe 8(7)]

Plainte

Un exécuteur testamentaire s'est plaint qu'une banque ait refusé d'acquiescer à sa demande de renseignements personnels concernant le coffre bancaire de sa tante décédée.

Résumé de l'enquête

Le plaignant soupçonnait qu'une certaine personne non autorisée avait, avec le concours des avocats de la succession, accédé au coffre bancaire de la tante décédée et pris des articles de valeur. Le plaignant avait recueilli un élément de preuve (c-à-d une réponse négative d'une succursale de la banque ayant été transmise par télécopieur) qui évoquait fortement la possibilité que la banque ait reçu des avocats au moins une demande indépendante se rapportant au portefeuille bancaire de la défunte. En sa qualité d'exécuteur testamentaire, le plaignant a demandé à la banque de consulter la carte de signatures pour le coffre bancaire et toute correspondance entre la banque et les avocats de la succession. La banque a répondu qu'il lui était impossible de trouver la carte ou les éléments de correspondance. La recherche approfondie dans les dossiers bancaires, qu'ont menée l'ombudsman de la banque, l'Ombudsman bancaire canadien et le Commissariat à la protection de la vie privée, n'a pas permis de trouver les renseignements demandés par le plaignant.

En temps normal, la banque conserve les cartes de signatures subordonnées aux coffres bancaires pendant sept ans. Huit jours après le décès de la tante, tous les coffres bancaires avaient été transférés d'une succursale bancaire à une autre, et les mesures de sécurité qui s'imposent avaient été appliquées au cours du transfert. La politique bancaire ne

prévoyait pas, toutefois, qu'une succursale conserve des dossiers sur un compte, un placement ou un coffre bancaire après leur transfert dans une autre succursale. La politique bancaire ne prévoyait pas plus qu'une succursale conserve des demandes de renseignements relatifs à un dossier qui ne s'y trouvait plus.

*Conclusions du Commissaire
(rendues le 12 octobre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.9 de l'annexe I précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation et de leur communication à des tiers, et lui permettre de les consulter. Le paragraphe 8(7) précise que l'organisation qui refuse, dans le délai prévu, d'acquiescer à la demande notifie par écrit au demandeur son refus motivé et l'informe des recours que lui accorde la présente partie.

Le Commissaire a établi que les renseignements que la banque n'a pu produire auraient dû être conservés conformément au principe énoncé à l'article 4.5, et n'auraient pas dû être

perdus. Par conséquent, il a jugé que la banque n'avait pas respecté le principe énoncé à l'article 4.9. Il a en outre jugé que la réponse de la banque constituait un refus aux termes du paragraphe 8(7).

Le Commissaire a donc conclu que la plainte était fondée.

AUTRES CONSIDÉRATIONS

Le Commissaire a recommandé que la banque révise ses pratiques relatives à la destruction des documents contenant des renseignements personnels et élabore une politique écrite portant sur la conservation de tels documents, conformément aux dispositions pertinentes de la *Loi*.

Un employé prétend que son employeur a communiqué sans son consentement des renseignements à une société de placement [paragraphe 7(3) et principes énoncés aux articles 4.3 et 4.5 de l'annexe 1]

Plainte

Un employé d'une grande entreprise s'est plaint que son employeur ait indûment communiqué des renseignements personnels le concernant et concernant d'autres employés, y compris de l'information relative aux primes en espèce, sans avoir obtenu le consentement des employés ou les en avoir informés au préalable, à une société de placement qui s'occupe d'un REER et d'un régime d'épargne offerts par l'entreprise.

Résumé de l'enquête

L'entreprise en question a reconnu qu'elle communique des renseignements personnels concernant ses employés, sans avoir obtenu leur consentement explicite, à la société de placement qui s'occupe du REER et du régime d'épargne pour les employés à salaire horaire. Les renseignements divulgués comprennent les numéros de registre de paie et d'identité personnelle, nom, adresse, numéro d'assurance sociale, état matrimonial, sexe, langue de prédilection, date d'entrée en fonction, date de naissance, service, code de groupe et code syndical de l'individu. En outre, l'entreprise avertit la société de placement lorsqu'elle attribue des primes en espèce, sans toutefois préciser le nom du bénéficiaire ou le montant de la prime. Le REER et le régime d'épargne ont été établis par l'entreprise en vue de respecter l'engagement passé avec le syndicat du personnel en vertu de la convention collective. L'entreprise paie la société de placement pour les services fournis dans le cadre du régime et ne communique pas de renseignements à la société de placement pour contrepartie, qu'elle soit monétaire ou autre.

Conclusions du Commissaire (rendues le 18 octobre 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique strictement aux entreprises fédérales et aux communications de renseignements

personnels pour contrepartie à l'extérieur d'une province. L'entreprise en question n'est pas une entreprise fédérale au sens de la *Loi*, et elle ne communique pas les renseignements personnels en cause à l'extérieur de la province pour contrepartie.

Le Commissaire a conclu qu'il n'était pas de son ressort de poursuivre l'enquête sur cette plainte.

Un demandeur affirme ne pas avoir reçu son rapport de solvabilité d'une agence d'évaluation [article 8]

Plainte

Un individu s'est plaint qu'une agence d'évaluation du crédit ait refusé d'acquiescer à sa demande de consulter son rapport de solvabilité.

Résumé de l'enquête

Le plaignant avait écrit à l'agence d'évaluation du crédit pour demander de consulter tout rapport de solvabilité le concernant que l'agence aurait conservé dans ses dossiers. Dans sa plainte, il a affirmé ne pas avoir reçu, par la suite, de réponse de l'agence. Le centre des relations avec la clientèle de l'agence compte six employés qui sont chargés de recevoir et de traiter les demandes d'accès conformément aux formalités établies. Suivant ces formalités, une demande d'un client n'est pas classée avant d'avoir été assortie à un rapport de solvabilité ayant été envoyé par la poste ou remis au client. La demande d'accès du plaignant, qui porte une note manuscrite

indiquant qu'une réponse a été envoyée à l'adresse exacte du plaignant 13 jours après la réception de sa demande, se trouve dans les dossiers du centre. Le dépôt de la réponse à la poste était également confirmé par renvoi à un registre informatisé et à un rapport de vérification établi par ordinateur. Le plaignant, à un moment donné, a admis qu'il était possible qu'il ait tout simplement négligé de remarquer le rapport de solvabilité lorsqu'il l'a reçu. Il a déclaré ultérieurement qu'il était fort improbable qu'il ait reçu le rapport sans le remarquer.

*Conclusions du Commissaire
(rendues le 26 octobre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique à toute communication de renseignements personnels pour contrepartie à l'extérieur d'une province. Cette plainte était du ressort du Commissaire parce que l'agence d'évaluation du crédit en question avait communiqué des renseignements personnels pour contrepartie à l'extérieur de la province.

APPLICATION : Le paragraphe 8(3) de la *Loi* précise que l'organisation saisie de la demande doit y donner suite avec la diligence voulue et, en tout état de cause, dans les trente jours suivant sa réception. Le paragraphe 8(5) précise que faute de répondre dans le délai, l'organisation est réputée avoir refusé d'acquiescer à la demande.

Le Commissaire n'a pas relevé de motif pour mettre en doute les éléments de preuve qui démontraient que l'agence d'évaluation du crédit avait reçu la demande d'accès du plaignant et lui avait envoyé une réponse par la poste dans le délai de réponse prescrit. Il a conclu que l'agence avait observé le paragraphe 8(3) de la *Loi*.

Le Commissaire a conclu que la plainte n'était pas fondée en vertu du paragraphe 8(5).

Une entreprise de transport aérien accusée de priver des voyageurs de leur droit de consulter des renseignements personnels au sujet d'incidents de voyage [principes énoncés aux articles 4.1 et 4.9 de l'annexe 1]

Plainte

Trois voyageurs aériens se sont plaints qu'une entreprise de transport aérien les ait privés de leur droit de consulter des renseignements personnels concernant leurs expériences au cours d'un voyage au Mexique.

Résumé de l'enquête

Les plaignants avaient demandé de consulter tous les renseignements personnels relatifs à certains événements qu'ils avaient vécus au cours d'un voyage au Mexique que détenaient l'entreprise de transport aérien et les services de voyage associés. Dans un premier temps, un représentant a répondu que l'entreprise n'était pas tenue de produire ces renseignements. Après que le Commissariat à la protection de la vie privée l'eut informée des

obligations auxquelles elle était liée en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, l'entreprise a aussitôt pris des mesures en vue de nommer un agent responsable de la conformité avec la *Loi*, a traité la demande d'accès des plaignants et leur a envoyé les renseignements personnels sur lesquels la demande portait. Les plaignants étaient d'avis, après avoir examiné ces renseignements, que l'entreprise n'avait pas joint les rapports d'incident. L'enquêteur pour le compte du Commissaire à la protection de la vie privée a examiné les dossiers originaux qui contenaient les renseignements personnels concernant les plaignants que détenait l'entreprise, mais rien n'indiquait qu'il existait des renseignements autres que ceux que les plaignants avaient déjà reçus. L'entreprise a confirmé par écrit qu'elle ne détenait pas d'autres renseignements au sujet des plaignants, y compris des rapports d'incident.

*Conclusions du Commissaire
(rendues le 31 octobre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *LPRPDÉ* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de transport aérien sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.1 de l'annexe I précise qu'une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect

[des principes stipulés à] l'annexe I. Le principe énoncé à l'article 4.9 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation et de leur communication, à des tiers, et lui permettre de les consulter.

En ce qui concerne le principe énoncé à l'article 4.1, le Commissaire a établi que l'entreprise de transport aérien n'avait pas désigné de responsable avant l'intervention du Commissariat. Par conséquent, il a jugé que l'entreprise, au départ, ne respectait pas ce principe. Néanmoins, il a également observé que l'entreprise avait depuis nommé un agent supérieur chargé d'assurer la conformité avec la *Loi*. Le Commissaire a jugé que cette question était réglée.

En ce qui concerne le principe énoncé à l'article 4.9, le Commissaire a établi que de nouveau, l'entreprise n'avait remis aux plaignants les renseignements personnels les concernant qu'après l'intervention du Commissariat. Par conséquent, il a jugé que l'entreprise, au départ, ne respectait pas ce principe. Il a toutefois observé que les plaignants étaient convaincus d'avoir reçu tous les renseignements personnels les concernant que l'entreprise détenait. De plus, les plaignants étaient satisfaits du résultat de l'enquête.

Le Commissaire a conclu que la plainte était fondée et résolue.

Une employée s'oppose à ce que son employeur inscrive son numéro de compte bancaire sur sa fiche de paie [principes énoncés aux articles 4.3 et 4.7 de l'annexe 1]

Plainte

Une employée d'une entreprise de télécommunications s'est plainte que son employeur :

1. ait utilisé des renseignements personnels la concernant à une fin à laquelle elle n'avait pas consenti en imprimant ses numéros de compte bancaire de domiciliation de la banque sur sa fiche de paie; et
2. n'ait pas protégé convenablement les fiches de paie du personnel, compte tenu du degré de sensibilité des renseignements qu'elles contiennent.

Résumé de l'enquête

Les employés de l'entreprise de télécommunications en question reçoivent leur paie par virement automatique, et leurs fiches de paie leur sont remises sous pli cacheté dans leur milieu de travail. En raison d'une fusion et de la conversion subséquente des systèmes de rémunération, les numéros de compte bancaire et de domiciliation de la banque sont inscrits sur les fiches de paie de tous les employés depuis le 1^{er} janvier 2001. L'impression de ces numéros sur les fiches de paie est devenue pratique courante dans les secteurs privé et public. Sur les fiches produites par cette entreprise, rien n'indique ce que désignent les numéros, et seules les personnes qui connaissent bien les codes d'information de la

banque sauraient ce qu'ils représentent. Les enveloppes cachetées contenant les fiches de rémunération du personnel, lorsqu'elles sont livrées au milieu de travail de la plaignante, sont réunies dans une plus grande enveloppe qui est déposée sur le bureau du gestionnaire, où il arrive souvent, au cours de périodes comptant jusqu'à 24 heures, qu'elle soit laissée à découvert et sans surveillance.

À l'origine, la plaignante avait consenti à ce que sa paie soit déposée directement dans son compte bancaire, mais elle n'a jamais donné son consentement explicite pour que ces numéros figurent sur sa fiche. C'est pourquoi elle a affirmé que son employeur utilisait des renseignements personnels concernant son compte bancaire sans son consentement et à une fin qui n'était pas compatible avec celle à laquelle elle avait fourni les renseignements au départ. De plus, elle a affirmé que son employeur ne protégeait pas convenablement les fiches de paie du personnel dans son milieu de travail.

L'entreprise a soutenu que les renseignements étaient bel et bien utilisés à la seule fin à laquelle ils avaient été recueillis, à savoir le virement automatique des paies; qu'il était désormais impératif, pour les besoins de la vérification de l'affectation des fonds salariaux et la résolution des écarts, d'imprimer les numéros de compte et de succursale sur les fiches de paie; et que bon nombre d'employés en étaient déjà venus à s'attendre à ce que ces

numéros soient inscrits sur leur fiche, et à s'y fier. De plus, l'entreprise a soutenu avoir protégé convenablement les renseignements relatifs aux comptes bancaires de ses employés, car elle distribuait les fiches sous pli confidentiel et cacheté.

*Conclusions du Commissaire
(rendues le 5 novembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. Ce principe stipule en outre (à l'article 4.3.5) que les attentes raisonnables de la personne sont pertinentes. Le principe énoncé à l'article 4.7 précise que les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Au sujet du premier élément de la plainte (consentement), le Commissaire a établi qu'il était raisonnable que les employés qui divulguent leurs numéros de compte bancaire et de domiciliation de la banque aux fins du

virement automatique s'attendent à ce que ces numéros figurent sur les fiches de transaction aux fins de la vérification de l'affectation des fonds, lesquelles correspondent tout à fait aux fins convenues. Il était donc d'avis que la plaignante avait donné son consentement implicite. Par conséquent, il a jugé que l'entreprise avait satisfait à ses obligations en vertu du principe énoncé à l'article 4.3 de l'annexe 1.

Le Commissaire a conclu qu'à cet égard, la plainte n'était pas fondée.

Au sujet du deuxième élément de la plainte (mesures de sécurité), le Commissaire a établi que les mesures de contrôle opérationnel appliquées par l'entreprise dans le milieu de travail de la plaignante ne correspondaient pas au degré de sensibilité des renseignements personnels contenus dans les fiches de paie. Il a jugé que l'entreprise avait manqué à ses obligations en vertu du principe énoncé à l'article 4.7 de l'annexe 1.

Il a toutefois observé que l'entreprise, après qu'elle eut été informée de ses obligations, avait pris immédiatement des mesures appropriées pour corriger ses pratiques de gestion de l'information relativement aux fiches de paie du personnel.

Le Commissaire a conclu qu'à cet égard, la plainte était fondée et résolue.

AUTRES CONSIDÉRATIONS

L'entreprise a convenu de mettre en œuvre, comme solution à court terme, des mesures de contrôle opérationnel plus rigoureuses dans le milieu de travail de la plaignante et d'offrir à la plaignante la possibilité de recevoir sa fiche de paie par la poste, à domicile.

Une entreprise demande le NAS d'une cliente en vertu d'une politique [principes énoncés aux articles 4.3.3 et 4.4.1 de l'annexe 1, et paragraphe 5(3)]

Plainte

Une particulière s'est plainte qu'une entreprise de télécommunications ait indûment recueilli des renseignements personnels la concernant, à savoir son numéro d'assurance sociale (NAS).

Résumé de l'enquête

L'entreprise de télécommunications en question avait demandé le NAS de la plaignante au moment de la conclusion d'une entente de service de connexion Internet avec elle. Aux dires de la plaignante, le représentant de l'entreprise avec qui elle s'était entretenue lui avait signifié que « sans NAS, pas de connexion », de sorte qu'elle s'était sentie obligée de donner son numéro pour recevoir le service. La collecte du NAS des clients éventuels était prévue par la politique écrite de l'entreprise. Cette politique visait à éviter que des similarités dans les noms des clients ne prêterent à confusion. Néanmoins, selon cette politique, l'entreprise ne devait pas insister pour connaître le NAS des clients qui

refusaient de le divulguer, et l'entreprise avait signalé à son personnel que la collecte n'était pas obligatoire.

Conclusions du Commissaire (rendues le 5 novembre 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3.3 de l'annexe 1 précise qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, 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 légitimes et explicitement indiquées. Le principe énoncé à l'article 4.4.1 précise que les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Le paragraphe 5(3) stipule que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En ce qui concerne le principe énoncé à l'article 4.4.1, le Commissaire a établi que, conformément à la politique de l'entreprise, la collecte des NAS n'était pas obligatoire et que, pour ce motif, elle n'était pas nécessaire pour réaliser les fins légitimes et explicitement indiquées. Par conséquent, il a jugé que la collecte était arbitraire et que l'entreprise contrevenait à ce principe.

En ce qui concerne le principe énoncé à l'article 4.3.3, le Commissaire était d'avis qu'on avait nettement donné l'impression à la plaignante que la divulgation de son NAS était une condition du service. Par conséquent, il a jugé que l'entreprise contrevenait à ce principe.

En ce qui concerne le paragraphe 5(3), le Commissaire s'est penché attentivement sur une position défendue depuis longtemps au Commissariat, selon laquelle il ne faudrait pas recourir au NAS comme à un identificateur universel et les citoyens ne devraient pas divulguer leur NAS à moins que la loi ne les y oblige pour la réalisation des fins d'un certain nombre de programmes fédéraux qui sont en droit de recueillir ces renseignements. Il était d'avis qu'une personne raisonnable s'opposerait à la collecte de NAS pour un service de connexion Internet. Par conséquent, il a jugé que l'entreprise contrevenait aux dispositions du paragraphe 5(3).

Le Commissaire a observé que l'entreprise avait supprimé le NAS en cause du dossier de la plaignante et qu'elle en était à modifier sa politique afin que les NAS ne soient plus demandés.

Le Commissaire a donc conclu que la plainte était fondée et résolue.

AUTRES CONSIDÉRATIONS

Le Commissaire a également recommandé que l'entreprise mette en œuvre une démarche d'examen de ses dossiers et qu'elle supprime tous les autres NAS ayant été inutilement recueillis auprès de ses clients.

Une utilisatrice accuse un FSI de lire ses messages électroniques et d'empêcher leur transmission [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Une particulière s'est plainte que son ancien fournisseur de services Internet (FSI) :

1. ait indûment recueilli des renseignements personnels la concernant, sans son consentement, du fait qu'il ait lu ses messages électroniques; et
2. ait empêché la transmission de messages électroniques qu'elle tentait d'envoyer à des utilisateurs de son ancien FSI par le biais d'un nouveau FSI.

Résumé de l'enquête

La plaignante avait été abonnée aux services d'un certain FSI pendant deux ans. Au cours de cette période, son utilisation du compte, et plus particulièrement, ses tentatives de transmission de fichiers volumineux par courrier électronique, avaient provoqué un conflit entre elle et le FSI. Elle a affirmé que le fournisseur lui avait alors dit pouvoir lire ses messages électroniques. Elle a en outre affirmé qu'après qu'elle eut déménagé dans une autre ville et souscrit un abonnement auprès d'un autre FSI, ce même fournisseur avait commencé à bloquer la transmission de messages électroniques qu'elle tentait de faire parvenir à des utilisateurs de son ancien FSI. Le fournisseur en question a déclaré qu'il ne se souvenait pas de s'être trouvé en désaccord avec la plaignante, mais il a admis que selon la pratique courante, à la découverte d'un grand nombre de messages « d'échec de remise » (signalant les tentatives de transmission de fichiers volumineux par courrier électronique), il aurait appelé l'utilisateur en cause afin de discuter de la question. Il a nié pouvoir lire des messages liés au compte de la plaignante à part ceux qui indiquent un « échec de remise ». Il a aussi nié avoir empêché la transmission des messages de la plaignante.

L'enquête a confirmé que le FSI en question peut surveiller les activités relatives aux comptes des utilisateurs et déceler les messages « d'échec de remise », mais qu'il ne reçoit pas de messages électroniques ou de pièces jointes et ne peut pas lire les messages électroniques des utilisateurs. En outre, il n'y avait pas d'élément de preuve indiquant que le fournisseur avait empêché la transmission des messages électroniques de la plaignante par son nouveau serveur. De fait, plusieurs semaines avant que le fournisseur ne soit avisé de la plainte déposée contre lui, le problème de transmission a cessé lorsqu'un technicien en informatique a modifié l'adresse IP de l'ordinateur de la plaignante.

Conclusions du Commissaire (rendues le 5 novembre 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les fournisseurs de services Internet sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3 de l'annexe I précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Le Commissaire était d'avis qu'il aurait été impossible au FSI de lire les messages électroniques de ses utilisateurs, et que le FSI n'avait pas empêché la transmission des messages de la plaignante. De plus, il a établi qu'une personne raisonnable s'attendrait à ce que le FSI surveille les services qu'il fournit et donne suite à des messages récurrents « d'échec de remise ». Il a conclu que dans cette affaire, le FSI ne contrevenait pas au principe énoncé à l'article 4.3 de l'annexe 1.

Le Commissaire a donc conclu que la plainte n'était pas fondée.

Un employeur envoie à des tiers des copies d'une réponse à des demandes d'accès présentées par une employée [principes énoncés aux articles 4.3 et 4.5 de l'annexe 1, et paragraphe 5(3)]

Plainte

Une employée d'une administration aéroportuaire s'est plainte que son employeur ait, sans son consentement, communiqué à des tiers des renseignements personnels la concernant en leur envoyant des copies d'une lettre de réponse à des demandes d'accès qu'elle avait présentées.

Résumé de l'enquête

La plaignante avait présenté des demandes d'accès, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, afin de consulter des renseignements que détenait son employeur.

L'employeur lui a par la suite envoyé une lettre de réponse qui indiquait que l'organisation rejetait ses demandes. La lettre indiquait en outre que des copies de la réponse seraient adressées à trois autres personnes : deux représentants syndicaux et le coordonnateur des relations avec les employés de l'aéroport. La plaignante n'avait pas fait parvenir de copies de ses demandes d'accès à ces parties et n'avait pas consenti explicitement à ce que des copies de la lettre de réponse leur soient envoyées.

Les représentants syndicaux avaient précédemment participé à une réunion au cours de laquelle la question de l'accès aux renseignements personnels concernant la plaignante avait été soulevée. Le coordonnateur des relations avec les employés était précédemment intervenu dans une plainte de harcèlement déposée par la même plaignante et il détenait certains des documents connexes qu'elle demandait à consulter. L'employeur a fait valoir que la plaignante avait donné son consentement implicite à la communication de ces renseignements à ces personnes suivant les motifs de ces interventions antérieures. La plaignante a soutenu qu'elle avait présenté les demandes d'accès personnellement et en son propre nom, sans le concours du syndicat.

*Conclusions du Commissaire
(rendues le 5 novembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les aéroports sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. Le principe énoncé à l'article 4.5 stipule que les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. Le paragraphe 5(3) précise que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En ce qui concerne le principe énoncé à l'article 4.3 et la communication des renseignements aux représentants syndicaux, le Commissaire a établi que l'employeur aurait été autorisé par consentement implicite à envoyer les copies de la réponse à ces parties seulement si la plaignante avait indiqué qu'elle leur avait fait parvenir des copies de

ses demandes d'accès. La plaignante était en droit d'exercer son recours officiel sans le concours du syndicat, et l'employeur n'était pas tenu d'informer le syndicat de sa réponse. Il a conclu qu'il n'y avait pas eu de consentement implicite se rapportant aux représentants syndicaux. En ce qui concerne le paragraphe 5(3), le Commissaire était d'avis qu'une personne raisonnable aurait estimé que la communication des renseignements aux représentants syndicaux était inacceptable.

Il a donc conclu que cet aspect de la plainte était fondé.

En ce qui concerne le principe énoncé à l'article 4.5 et le coordonnateur des relations avec les employés, compte tenu de la participation directe de cette personne dans la demande d'accès, le Commissaire a établi qu'il était approprié que l'employeur informe le coordonnateur de sa décision de refuser d'acquiescer à la demande d'accès à des documents présentée par la plaignante. En ce qui concerne le paragraphe 5(3), le Commissaire était d'avis qu'une personne raisonnable aurait estimé que la communication des renseignements au coordonnateur des relations avec les employés était acceptable. Il a conclu que l'employeur s'est conformé au principe énoncé à l'article 4.5 concernant la question du coordonnateur des relations avec les employés.

Il a donc conclu que cet aspect de la plainte n'était pas fondé.

AUTRES CONSIDÉRATIONS

Au cours de l'enquête, le Commissariat à la protection de la vie privée a signalé à l'administration aéroportuaire en question qu'il est préférable de ne pas faire parvenir à des tiers des copies des réponses et qu'il faut plutôt laisser le soin à chaque demandeur de déterminer s'il souhaite faire connaître ces réponses à d'autres personnes après l'avoir reçue. Le Commissaire s'est réjoui de constater que l'organisation avait suivi ses conseils pour traiter des demandes d'accès présentées subséquemment par la plaignante.

Une entreprise de téléphone demande des pièces d'identité aux nouveaux abonnés [principes énoncés aux articles 4.2 et 4.2.3 et aux articles 4.3, 4.3.2 et 4.3.3 de l'annexe 1, et paragraphe 5(3)]

Plainte

Une particulière s'est plainte qu'une entreprise de télécommunications ait indûment recueilli des renseignements personnels auprès de nouveaux abonnés en exigeant que ses nouveaux clients qui refusent de produire ces renseignements versent un acompte.

Résumé de l'enquête

Lorsque la plaignante a tenté de s'abonner à un nouveau service téléphonique auprès de l'entreprise en question, un téléphoniste lui a demandé de produire deux pièces d'identité. La plaignante s'est montrée hésitante, et le téléphoniste lui a dit que si elle refusait de le faire, elle devrait verser un acompte. Le téléphoniste lui a aussi dit que la collecte de ces renseignements visait à confirmer son identité. Le superviseur de l'entreprise lui a subséquemment expliqué la collecte de la même façon, et a confirmé qu'à défaut de produire ces renseignements, la plaignante devrait verser un acompte.

La politique de l'entreprise prévoit que les téléphonistes doivent demander aux nouveaux abonnés de produire deux pièces d'identité, exiger un acompte en cas de refus, et expliquer que la collecte de ces renseignements vise tout simplement à confirmer l'identité de l'abonné. Toutefois, lorsque le demandeur est un nouveau client qui n'a jamais fait affaire avec l'entreprise, la collecte a pour véritable objet de procéder à la vérification du crédit de cette personne, conformément aux règlements du CRTC, étant donné que l'entreprise, lorsqu'elle fournit des services téléphoniques, accorde un crédit à l'utilisateur.

*Conclusions du Commissaire
(rendues le 8 novembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le principe énoncé à l'article 4.2.3 stipule que les fins auxquelles les renseignements sont destinés doivent être précisées avant la collecte ou au moment de celle-ci. Le principe énoncé à l'article 4.3.2 précise que les organisations doivent faire un effort raisonnable pour informer la personne concernée des fins auxquelles les renseignements seront utilisés et pour énoncer les fins de façon que la personne puisse raisonnablement les comprendre. Le principe énoncé à l'article 4.3.3 stipule qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que celles qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées. Le paragraphe 5(3) précise que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En ce qui concerne le principe énoncé à l'article 4.3.3 et le paragraphe 5(3), le Commissaire a établi qu'une personne raisonnable estimerait qu'il est acceptable que l'entreprise recueille des renseignements personnels pour les besoins de la confirmation de la solvabilité des clients éventuels ou, lorsqu'il s'agit de clients réguliers, de la confirmation de leur identité.

Il a conclu qu'à cet égard, la plainte n'était pas fondée.

En ce qui concerne les principes énoncés aux articles 4.2.3 et 4.3.2, le Commissaire a établi qu'une personne raisonnable conclurait que l'entreprise n'avait pas exposé explicitement l'objet de sa collecte de renseignements personnels concernant les nouveaux abonnés.

Il a conclu qu'à cet égard, la plainte était fondée.

AUTRES CONSIDÉRATIONS

L'entreprise a convenu de modifier sa pratique et d'exposer les fins de la collecte. Plus particulièrement, l'entreprise avisera les nouveaux abonnés que la collecte de renseignements vise à évaluer leur solvabilité, étant donné que l'entreprise fait crédit à l'utilisateur lorsqu'elle lui fournit un service interurbain.

Un radiodiffuseur accusé de recueillir des renseignements personnels sur son site Web [article 2, et principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Un particulier s'est plaint qu'un radiodiffuseur ait tenté de recueillir, au moyen de son serveur publicitaire, des renseignements personnels qui le concernent, à savoir l'information NetBIOS de son ordinateur, sans avoir obtenu son consentement.

Résumé de l'enquête

Le plaignant avait un ordinateur équipé d'un modem câble pour la connexion Internet et d'un garde-barrière pour la détection et le rejet des tentatives d'intrusion. Chaque fois que le plaignant essayait d'entrer en communication avec le site Web de l'organisation, son garde-barrière détectait et rejetait une démarche de collecte de l'information NetBIOS de son ordinateur lancée par le serveur publicitaire de l'organisation, puis produisait un rapport à ce sujet. NetBIOS est le nom courant ou « convivial » désignant un ordinateur suivant à son adresse IP.

Le dépistage d'une adresse IP permet d'avoir accès à des renseignements comme les sites Web qu'a visités l'utilisateur de l'ordinateur ou les mots de passe qu'il a utilisés récemment pour consulter des comptes protégés. Lorsqu'un utilisateur a accès à Internet par

réseau commuté, la probabilité que l'adresse IP de son ordinateur soit dépistée est faible, mais celle-ci est beaucoup plus élevée si l'utilisateur a une connexion Internet permanente par modem câble, comme dans le cas du plaignant.

Après avoir mené des enquêtes à l'interne, le radiodiffuseur a ajouté foi à la prétention du plaignant. Le radiodiffuseur a expliqué que le gestionnaire de réseau, au moment d'installer Windows NT de Microsoft, avait négligé de désactiver certaines caractéristiques qui accompagnent le programme. Lorsque ces caractéristiques, qu'on appelle service WIMS, sont en fonction, le serveur peut recueillir l'information NetBIOS des utilisateurs du site Web. Le gestionnaire du réseau, après avoir appris que les caractéristiques étaient en fonction, les a désactivées sans tarder. Le plaignant a confirmé par la suite que son garde-barrière ne relevait plus de tentative de collecte de l'information NetBIOS attribuable par l'organisation.

Conclusions du Commissaire (rendues le 20 novembre 2001)

COMPÉTENCE : Depuis le 1^{er} janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les radiodiffuseurs sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Selon l'article 2 de la *Loi*, un renseignement personnel se dit de « [...] tout renseignement concernant un individu identifiable [...] » Le principe énoncé à l'article 4.3 de l'annexe I précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Le Commissaire était d'avis que dans certaines circonstances, comme la situation du plaignant, l'information NetBIOS peut servir à recueillir des renseignements qui peuvent être liés à un individu identifiable. Il a donc établi que les renseignements en cause étaient considérés comme personnels aux fins de la *Loi*.

Le Commissaire a conclu que le radiodiffuseur avait manqué à ses obligations en vertu du principe énoncé à l'article 4.3. Il n'a toutefois pas contesté l'explication de l'organisation selon laquelle le manquement était involontaire, il a fait observer qu'il avait pris des mesures satisfaisantes.

Il a donc conclu que la plainte était fondée et résolue.

Un couple prétend que la banque lui a refusé l'accès à des renseignements sur une demande de prêt [paragraphe 8(3) et 8(5)]

Deux plaintes

Un couple s'est plaint dans deux cas distincts qu'une banque leur ait refusé l'accès à des renseignements personnels le concernant, car elle n'a pas répondu à une demande d'information relative à une demande de prêt.

Résumé de l'enquête

Les plaignants avaient rédigé et présenté deux lettres, portant leur signature, pour demander des renseignements personnels relatifs à deux produits de crédit distincts qu'offrait la succursale locale de la banque en question. Les lettres étaient presque identiques, seules les lignes de mention objet les distinguaient, l'une indiquant un numéro de demande de prêt et l'autre, un numéro de prêt hypothécaire, toutes deux concernaient les deux plaignants. Au cours du mois suivant, la banque leur a fait parvenir les renseignements qu'ils avaient demandés au sujet de leur prêt hypothécaire, mais pas ceux ayant trait à leur demande de prêt. Les plaignants ont envoyé à la banque une autre lettre qui décrivait plus en détail les renseignements qu'ils voulaient obtenir au sujet de leur demande de prêt. Environ un mois après la soumission de la deuxième lettre, un avocat de la banque a

répondu aux plaignants en leur indiquant seulement qu'ils devraient couvrir les frais de photocopie, à raison de 25 cents la page. Les plaignants ont alors envoyé une autre lettre, à laquelle ils ont joint un chèque au montant des frais de photocopie, qui confirmait qu'ils souhaitaient toujours obtenir les renseignements demandés. Trois semaines après l'envoi de la lettre, ils n'avaient toujours pas reçu de réponse, et ils ont déposé une plainte auprès du Commissariat à la protection de la vie privée.

La banque a d'abord nié l'allégation, soutenant que la deuxième demande des plaignants était la première qui traitait de la demande de prêt. Toutefois, après qu'on lui ait présenté une copie de la première lettre portant sur la demande de prêt, la banque a vérifié ses dossiers puis a reconnu l'avoir reçue. La banque a expliqué qu'elle n'avait pas délibérément choisi de ne pas répondre à cette demande, mais que l'employé qui avait reçu la première lettre, n'avait pas relevé les lignes de mention objet différentes des deux lettres, et avait tenu pour acquis qu'elles étaient identiques. C'est pourquoi l'employé n'avait fait suivre que l'une des lettres (celle traitant du prêt hypothécaire).

*Conclusions du Commissaire
(rendues le 26 novembre 2001)*

COMPÉTENCE : Depuis le 1^{er} janvier 2001, les entreprises fédérales tombent sous le coup de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

APPLICATION : Le paragraphe 8(3) de la *Loi* porte ce qui suit que l'organisation saisie de la demande doit y donner suite avec la diligence voulue et, en tout état de cause, dans les trente jours suivant sa réception. Le paragraphe 8(5) précise que faute de répondre dans le délai, l'organisation est réputée avoir refusé d'acquiescer à la demande.

Le Commissaire a conclu que la banque n'avait pas répondu dans le délai et contrevenait par conséquent à l'article 8. Il était toutefois d'avis que ce manquement était involontaire, et il a observé que par la suite, la banque avait fourni aux plaignants tous les renseignements visés par leur demande.

Il a donc conclu que les plaintes étaient fondées et résolues.

Incidents en vertu de la *LPRPDE*

Les incidents sont des affaires qui sont portées à mon attention par diverses sources, notamment des questions soulevées dans les médias. Il s'agit habituellement de situations dans lesquelles aucune victime n'a été identifiée et pour lesquelles aucune plainte n'a été déposée. Au cours des onze derniers mois, le Commissariat s'est penché sur les deux incidents suivants.

Une entreprise de transport recueille et communique des renseignements personnels concernant les passagers

Incident

On a prétendu que les agents de vente d'une compagnie de transport :

1. demandaient aux individus qui faisaient des réservations de billets de train au téléphone ou en personne pour le trajet Toronto-New York de divulguer leur date de naissance, leur citoyenneté et leur nom;
2. et communiquaient ces renseignements au Service des douanes américaines et au Service d'immigration et de naturalisation des États-Unis.

Résumé de l'enquête

L'entreprise a confirmé que la pratique en question avait lieu depuis décembre 2000, suivant une entente conclue entre l'entreprise de transport américaine, l'Agence canadienne

des douanes et du revenu, et le Service des douanes américaines et le Service d'immigration et de naturalisation des États-Unis. Cette pratique vise à écourter l'attente à la frontière canado-américaine. De plus, les renseignements personnels recueillis à cette fin sont stockés dans le système informatique de réservation de l'entreprise et en sont supprimés si l'individu, finalement, n'achète pas de billet. Lorsque le passager achète de billet, ses nom, date de naissance et citoyenneté sont imprimés sur un manifeste, qui est ensuite transmis par télécopieur au Service des douanes américaines et au Service d'immigration et de naturalisation des États-Unis, et dont une copie est remise au directeur des services à bord du train. Le directeur des services détruit le manifeste peu après la fin du voyage.

Le Commissariat à la protection de la vie privée du Canada a établi que les agents de vente, à la demande écrite de l'entreprise, avaient présenté cette pratique comme une exigence à laquelle les passagers du trajet Toronto-New York devaient satisfaire.

Résultat

L'entreprise a demandé conseil au Commissariat à la protection de la vie privée du Canada quant à la façon de résoudre le problème de façon satisfaisante. Le Commissariat a recommandé à l'entreprise de communiquer à ses agents de vente des directives claires

selon lesquelles la communication de la date de naissance et de la citoyenneté est volontaire, et que les agents peuvent, après la réservation des billets, demander aux clients s'ils acceptent de divulguer ces renseignements en vue de faciliter les formalités douanières à la frontière.

Le Commissariat, après avoir reçu une copie des directives transmise par l'entreprise aux agents de vente, a informé l'entreprise que le dossier d'incident serait fermé, sous réserve de la surveillance continue des pratiques de réservation des agents de vente. En outre, le Commissariat a recommandé que l'entreprise envoie à tous ses agents, à un moment donné, une note de suivi établissant encore plus clairement qu'ils ne doivent pas recueillir de renseignements personnels au moment de la réservation sans le consentement éclairé de l'individu.

Un site Web diffuse des conversations par téléphones cellulaires

Incident

Le 7 juin 2001, le *Ottawa Sun* a publié un reportage selon lequel un site Web à Ottawa retransmettait sur Internet des conversations par téléphones cellulaires.

Un scanner interceptait des communications téléphoniques cellulaires. Il était relié à l'ordinateur hôte d'un site Web. Quiconque visitait le site Web pouvait écouter des conversations téléphoniques privées.

Résultat

Lorsque le Commissariat à la protection de la vie privée du Canada a lancé son enquête, le fournisseur de services Internet (FSI) en question a fermé le site Web en raison de problèmes de largeur de bande. Les problèmes étaient imputables à un employé qui, ayant son propre compte de réseau, transmettait des données par un autre serveur. Lorsqu'il a découvert ses activités, le FSI a immédiatement relevé l'employé de ses fonctions. Le FSI a indiqué que le site Web en question avait été transféré à un serveur de New York, sous une nouvelle direction.

Étant donné qu'on a fermé le site Web à Ottawa, l'enquête du Commissariat a été abandonnée. Le site Web sera surveillé périodiquement pendant une période indéterminée.

Genres d'enquête en vertu de la LPRPDÉ
1^{er} janvier 2001 - 30 novembre 2001

Objet	Nombre
Dossiers criminels	30
Tests de dépistage de drogues	3
Chiffrement de données	7
Institutions fédérales	1 519
Vol d'identité	38
Demandes de renseignements	2 558
Interception – surveillance	154
Interprétation	2 024
Secteur de compétence	1 975
Marketing	439
Dossiers médicaux	137
Appels de députés	7
Demandes de publication	675
Numéro d'assurance sociale	1 834
Télécommunications	786
Transports	139
Autres	388
Total	12 713

PRATIQUES ET EXAMENS EN MATIÈRE DE VIE PRIVÉE

Aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*, je suis autorisé à procéder à la vérification de la conformité des organisations privées dans la mesure où j'ai des « motifs raisonnables de croire » que celles-ci contreviennent à une disposition de la *Loi*.

Suivant les objectifs et les critères de vérification normalisés communément acceptés, la Direction des Examens et des pratiques en matière de vie privée du Commissariat effectue les examens et les vérifications de conformité aux termes de l'article 18 de la *Loi*. Comme la *Loi* n'est entrée en vigueur qu'au début de 2001, je n'ai toujours pas eu l'occasion d'effectuer de telle vérification. Mes efforts ont plutôt porté sur la sensibilisation des entreprises et des organisations à l'incidence de la nouvelle *Loi*, et j'ai tâché de leur donner des conseils pour qu'elles mettent en place des politiques en matière de vie privée qui soient conformes à la *Loi*.

DEVANT LES TRIBUNAUX

Mathew Englander c. Telus Communications Inc.

Il s'agit de la première demande de révision judiciaire déposée devant la Cour fédérale en vertu de la *LPRPDÉ*. Le 1^{er} janvier 2001, Mathew Englander a déposé une plainte auprès du Commissariat à la protection de la vie privée, dans laquelle il prétendait, entre autres choses, que Telus utilise et communique les nom, adresse et numéro de téléphone des consommateurs, à leur insu et sans leur consentement, pour les pages blanches de l'entreprise et à d'autres fins, et que Telus exige indûment des frais de service aux consommateurs qui choisissent la « non-publication » de leur numéro de téléphone. Selon le demandeur, ces mesures de Telus contreviennent aux paragraphes 5(1) et (3) de la *LPRPDÉ* et à plusieurs articles de l'annexe 1 de la *LPRPDÉ*.

Après avoir fait enquête sur la plainte, j'ai conclu que Telus est tout à fait conforme à la *Loi* concernant les motifs de la plainte, et qu'une personne raisonnable estimerait que Telus dans sa pratique d'initiation de service et la publication subséquente, dans les pages blanches de Telus, des renseignements personnels des consommateurs représentent une collecte, une utilisation et une communication indiquées de renseignements. J'ai en outre conclu que l'entreprise est autorisée à

exiger des frais à ses consommateurs pour un service de numéro non publié, et qu'il ne s'agit pas d'une pratique abusive qui contrevient au principe énoncé à l'article 4.3.3 de l'annexe 1.

Par conséquent, j'ai conclu que la plainte n'était pas fondée. M. Englander a demandé l'audition de la question devant la Cour, comme l'autorise l'article 14 de la *LPRPDÉ*.

Ronald G. Maheu c. le Procureur général du Canada et IMS Health Canada

Le demandeur a présenté une demande d'audition devant la Cour fédérale, comme l'autorise l'article 14 de la *LPRPDÉ*, après s'être plaint, auprès du Commissariat, que IMS Health ait communiqué à tort des renseignements personnels en recueillant et en vendant des données relatives aux habitudes de prescription des médecins sans leur consentement.

Après avoir fait enquête dans cette affaire, j'ai conclu que les renseignements sur les ordonnances, que ce soit sous forme d'ordonnances individuelles ou sous forme de tendances dégagées d'un certain nombre d'ordonnances, ne sont pas des renseignements personnels concernant un médecin. Touchant la question à savoir si les renseignements en cause étaient des renseignements personnels au sens et selon

la portée et l'objet de la *Loi*, j'étais d'avis que le sens de « renseignement personnel », bien que vaste, ne l'est pas assez pour englober tous les renseignements associés à un individu. J'ai estimé que l'ordonnance individuelle, quoiqu'elle puisse révéler des renseignements au sujet d'un patient, n'est pas, de façon significative, un renseignement concernant le médecin prescripteur en tant qu'individu, mais qu'elle concerne plutôt le processus professionnel qui a débouché sur la délivrance de l'ordonnance, et qu'il faudrait considérer que l'ordonnance est un produit de travail, c'est-à-dire le résultat tangible de l'activité de travail du médecin. En somme, j'ai conclu que la plainte n'était pas fondée.

M. Maheu a présenté une demande d'audition devant la Cour. L'avis de demande comprenait une requête formulée par le demandeur, en vertu des règles de la Cour fédérale, pour que des documents détenus au Commissariat soient envoyés au demandeur et au Greffe de la Cour fédérale. Le Commissariat à la protection de la vie privée a refusé d'acquiescer à cette demande au motif que le Commissaire ne peut pas divulguer des documents qui ne sont pas déjà en la possession du demandeur, conformément aux dispositions de la *LPRPDÉ*.

COMMUNICATIONS ET SENSIBILISATION DU PUBLIC

Aux termes de la *LPRPDÉ*, le Commissariat a été mandaté pour sensibiliser le public aux questions touchant la vie privée de façon à accroître sa connaissance et sa compréhension de ces questions. Pour donner suite à cette importante nouvelle responsabilité, l'établissement de la Direction des communications et des analyses stratégiques a été une des premières initiatives que j'ai entreprise suivant mon entrée en fonction. La Direction a réalisé un nombre d'activités l'an dernier pour sensibiliser davantage aux questions touchant la vie privée et pour renseigner les entreprises et les citoyens canadiens sur la nouvelle *Loi* visant le secteur privé.

L'art oratoire est un outil inestimable que j'emploie pour m'acquitter de mes responsabilités liées à la promotion et à la sensibilisation auprès du public concernant les questions de vie privée. J'ai prononcé 35 allocutions à un vaste éventail d'organisations partout au Canada et à l'étranger au cours de l'an dernier. Les cadres supérieurs du Commissariat ont prononcé 31 autres discours. Ces discours ont porté sur les principales questions d'actualité, comme la controverse entourant la sécurité et la vie privée qui a fait suite aux attaques du 11 septembre aux États-Unis. De nombreuses autres allocutions ont présenté une occasion de renseigner les citoyens et les entreprises sur la nouvelle *Loi* et son incidence, de discuter de la vie privée en

milieu de travail, et de faire part des préoccupations en matière de vie privée touchant des initiatives particulières, y compris Gouvernement en direct, les dossiers électroniques en matière de santé et l'usage accru de la surveillance vidéo.

De plus, en raison de l'influence exercée par les médias sur les sujets abordés lors de débats publics et de la sensibilisation accrue du public, le Commissariat a commencé à assurer un suivi proactif des questions touchant la vie privée abordées dans les médias, et je me suis davantage engagé dans diverses activités de relations avec les médias.

Ces activités comprennent des déclarations publiques, la diffusion de communiqués et d'articles de fond à la fois aux médias grand public et spécialisés; les entrevues avec les médias et la rencontre des comités de rédaction des médias et le soutien des relations avec les médias relativement aux discours, aux conférences et à d'autres événements spéciaux. De plus, le Commissariat répond à des demandes de renseignements des médias, faisant des observations et donnant des renseignements généraux touchant une vaste gamme de questions liées à la vie privée.

Le nombre de demandes de renseignements s'accroît tous les mois, et il est actuellement de 80 à 100 par mois en moyenne. En outre, j'ai accordé plus de 210 entrevues aux médias depuis septembre 2000.

Documents de sensibilisation du public

Le Commissariat a élaboré et diffusé des documents promotionnels et de sensibilisation en réponse à la grande demande de renseignements sur la *LPRPDÉ*. Nous avons publié des guides complets sur la nouvelle *Loi* à l'intention des entreprises et des individus. Plus de 21 000 exemplaires de ces deux guides ont été distribués au cours de l'année 2001.

De plus, nous avons conçu des affiches, des trousseaux en matière de vie privée, des bloc-notes et des signets. Tous ces documents répondent à la demande de renseignements sur les questions liées à la vie privée présentées par les individus, les entreprises et d'autres organisations.

Publicité

Dans le cadre du programme de rayonnement, qui vise à sensibiliser aux droits à la vie privée des Canadiens et Canadiennes dans le secteur privé concernant tout d'abord les entreprises réglementées par le fédéral, le Commissariat a fait paraître des publicités dans plus de 1 300 quotidiens et journaux communautaires dans toutes les régions du Canada. L'objet de ces publicités était de renseigner les Canadiens et les Canadiennes sur leurs droits aux termes de la *LPRPDÉ*. La campagne publicitaire, dont le thème était, *Your privacy is our concern – Votre vie privée, ça nous regarde*, qui a été diffusée en mars 2001, a joint des millions de Canadiens et Canadiennes dans tous les coins du pays.

Une deuxième publicité est parue dans 12 quotidiens sur les trois territoires, signalant que la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique à toutes les entreprises territoriales qui sont considérées comme des entreprises fédérales. Suivant la parution de ces publicités, le Commissariat a pris note de l'accroissement du nombre de demandes de renseignements sur la *LPRPDÉ*.

Site Web

L'an dernier, le site Web du Commissariat a fait l'objet d'une reconception en profondeur et a été beaucoup élargi afin de donner suite au mandat de sensibilisation du public à la nouvelle *Loi*.

De nombreux efforts ont été déployés afin d'assurer que le site Web soit une ressource à jour concernant la protection des renseignements personnels ainsi qu'un outil de recherche utile sur les questions liées à la vie privée. En bout de ligne, le site Web de facture nouvelle est plus interactif, convivial et pertinent à la fois pour les individus et les entreprises.

Je suis heureux d'indiquer que le site Web est un outil de plus en plus efficace pour joindre les Canadiens et les Canadiennes et d'autres personnes, et sert à les renseigner sur les questions liées à la vie privée. Le nombre de visites du site continue d'augmenter, qui s'élève en moyenne à 11 500 par mois.

Activités de communication

1^{er} janvier 2001 - 30 novembre 2001

Activité	Nombre
Allocutions prononcées par le Commissaire à la protection de la vie privée	35
Allocutions prononcées par les cadres supérieurs	31
Communiqués	15
Entrevues avec les médias	210
Documents distribués	27 586
Guide à l'intention des entreprises	13 005
Guide à l'intention des citoyens	8 707
Autres (rapports annuels, signets, feuilles de renseignements, lois, etc.)	5 874
Nombre moyen de visites du site Web par mois	11 500



TROISIÈME PARTIE

SERVICES

DE GESTION

PRÉPARATIFS POUR LA MISE EN ŒUVRE DE LA LOI POUR LE SECTEUR PRIVÉ

Le Commissariat a ajouté à son personnel et accru son budget pour se préparer à la mise en œuvre de la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui est entrée en vigueur le 1^{er} janvier 2001.

Notre budget a été augmenté, passant à plus de 11 millions de dollars par année à compter du 1^{er} avril 2001; il était de 8,7 millions durant l'exercice 2000-2001. Cette augmentation budgétaire permettra au Commissariat d'apporter de nombreux changements importants, y compris les suivants :

- accroître le personnel affecté aux demandes de renseignements afin de pouvoir répondre aux appels plus nombreux;

- prolonger les heures d'affaires, de 9 h à 17 h, dans tous les fuseaux horaires du Canada;
- établir la Direction des Examens et des pratiques en matière de protection des renseignements personnels, qui se chargera des vérifications aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* et qui poursuivra le travail effectué dans le secteur privé;
- établir la Direction des communications et des analyses stratégiques, qui se chargera de l'actuelle fonction de recherche, de façon à focaliser les communications et la sensibilisation du public et à faire en sorte que nous soyons un centre de connaissances spécialisées sur les questions relatives à la vie privée;
- ajouter au nombre d'enquêteurs qui traiteront les plaintes aux termes des deux lois.

Un cadre financier à long terme touchant le financement futur sera présenté au Secrétariat du Conseil du Trésor du Canada en 2003-2004.

Ressources

(1^{er} avril 2000 - 31 mars 2001)

	ETP	Dépenses globales	Pourcentage du total
Vie privée	56	7 418 451 \$	89 %
Services de gestion	10	941 369 \$	11 %
Total	66	8 359 820 \$	100 %

Nota : Par ETP, on entend « équivalent temps plein » ou le personnel à temps plein.

Dépenses détaillées¹*1^{er} avril 2000 - 31 mars 2001*

	Vie privée	Services de gestion ²	Total
Salaires et traitements	3 776 280 \$	464 091 \$	4 240 371 \$
Cotisations au régime d'avantages sociaux des employés	611 000	84 500	695 500
Transports et communications	268 588	93 470	362 058
Information	979 136	1 993	981 129
Services professionnels	600 427	121 197	721 624
Location	33 036	13 958	46 994
Réparations et entretien	327 711	32 721	360 432
Matériel et fournitures	62 616	28 400	91 016
Acquisition de machines et d'équipements	759 403	100 998	860 401
Autres subventions et paiements	254	41	295
Total	7 418 451 \$	941 369 \$	8 359 820 \$

Nota :

¹ Les dépenses ne comprennent pas les redressements finals de fin d'exercice.² Les dépenses des Services de gestion sont également partagées entre le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information du Canada.

STRUCTURE ORGANISATIONNELLE

Commissariat à la protection de la vie privée du Canada

