Commissariat
à la protection de
la vie privée du Canada

LPRPDÉ

Tracer le chemin

Principaux développements au cours des sept premières années d'application de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ)

2008

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

613-995-8210, 1-800-282-1376
Téléc. : 613-947-6850
ATS : 613-992-9190

N° de cat. : IP54-6/2008
ISBN : 978-0-662-05731-4

Cette publication se trouve également sur notre site Web à www.privcom.gc.ca.

MESSAGE

Lorsque la *Loi sur la protection des renseignements personnels et les documents électroniques,* ou LPRPDÉ, a reçu la sanction royale en 2000, il était évident qu'on avait besoin de lois sur la protection des renseignements personnels s'appliquant au secteur privé : les Canadiennes et Canadiens réclamaient une protection adéquate de leurs renseignements personnels dans le cadre de la nouvelle économie numérique. Lors des débats ayant mené à l'adoption de la Loi, John Manley, alors ministre de l'Industrie, a déclaré à la Chambre des communes : « Que nous soyons consommateur, entreprise ou gouvernement, nous avons tous besoin d'avoir confiance dans la façon dont les renseignements personnels qui nous concernent sont recueillis, conservés et utilisés. La protection de notre vie privée est un droit élémentaire que les Canadiens et les Canadiennes chérissent. »

Depuis l'entrée en vigueur de la Loi, les organisations adaptent leurs pratiques commerciales afin de se conformer à la LPRPDÉ et aux normes provinciales similaires alors que leurs clients s'inquiètent de plus en plus au sujet de la protection de leurs renseignements personnels. Entre-temps, le contexte de la protection de la vie privée continue d'évoluer. Les progrès en technologie de l'information et le désir des entreprises de soutenir la concurrence à l'échelle mondiale ont plus que jamais complexifié les défis liés à la protection de la vie privée.

La compréhension qu'a le Commissariat de l'interprétation et de l'application de la Loi continue également d'évoluer. Au cours des sept dernières années, nous avons procédé à l'examen de plus de 2 600 plaintes individuelles et avons rendu des conclusions sur plusieurs enjeux découlant de la Loi et établissant des précédents. Le mécanisme de plaintes nous a permis d'obtenir un aperçu du fonctionnement de la LPRPDÉ en pratique.

Tracer le chemin a pour but de partager la compréhension que nous avons développée depuis la création de la Loi, en soulignant les conclusions de certaines enquêtes types touchant nombre d'enjeux importants. Les enjeux décrits dans ce rapport reflètent les inquiétudes actuelles et croissantes, tant des entreprises que de leurs clients, comme la surveillance croissante, la circulation transfrontalière des données, l'incidence des atteintes à la protection des données et la prolifération de l'utilisation des renseignements recueillis à des fins secondaires de marketing. Nous espérons que ce document contribuera à guider les entreprises dans l'élaboration et l'application de leurs propres pratiques de protection des renseignements personnels, en leur permettant de se fonder sur l'expérience des autres.

Plusieurs des conclusions soulignées dans ce document ont été rendues par l'ancienne commissaire adjointe, Heather Black, qui a pris sa retraite l'année dernière. Nous lui témoignons toute notre gratitude pour son travail de pionnière concernant l'adoption, la mise en œuvre et l'évolution de la Loi durant ses premières années cruciales, d'abord en tant qu'avocate générale puis en tant que commissaire adjointe responsable de la LPRPDÉ. Nous tenons à exprimer nos remerciements sincères à Heather et à reconnaître ses contributions importantes pour la progression du droit à la vie privée au Canada.

Nous souhaitons également remercier Alex Cameron de Fasken Martineau, que nous avons chargé de rédiger les premières ébauches de *Tracer le chemin*, ainsi que Patricia Kosseim, avocate générale au Commissariat, Ann Goldsmith, chef d'équipe des politiques, et le personnel de l'équipe des Communications qui a mené ce projet de sa conception à sa conclusion.

Jennifer Stoddart
Commissaire à la protection
de la vie privée du Canada

Elizabeth Denham
Commissaire adjointe à la protection
de la vie privée du Canada

TABLE DES MATIÈRES

INTRODUCTION

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) a été progressivement mise en œuvre sur une période de trois ans à partir du 1er janvier 2001.

La LPRPDÉ s'applique à toute organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans le cadre de ses activités commerciales[1]. Elle s'applique également aux installations, ouvrages, entreprises ou secteurs d'activité de compétence fédérale à l'égard des renseignements personnels qui concernent les employés et qui sont recueillis, utilisés ou communiqués dans le cadre de leur fonctionnement, qu'ils exercent des activités commerciales ou non[2].

La LPRPDÉ ne s'applique pas à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique en Alberta, en Colombie-Britannique ou au Québec (ou en Ontario, à l'égard des renseignements personnels sur la santé recueillis, utilisés ou communiqués par les dépositaires de renseignements sur la santé régis par la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario[3]), sauf :

1) si l'organisation est une installation, un ouvrage, une entreprise ou un secteur d'activité de compétence fédérale;

2) si les renseignements personnels sont communiqués en dehors de la province dans le cadre d'une activité commerciale.

Ces provinces ont édicté des lois sur la protection de la vie privée qui ont été déclarées essentiellement similaires à la LPRPDÉ[4]. En conséquence, la collecte, l'utilisation et la communication de renseignements personnels par des organisations dans le cadre d'activités commerciales dans ces provinces sont assujetties aux lois provinciales

1 Il est question du concept d'« activité commerciale » dans la partie 1 de ce document.

2 LPRPDÉ, alinéa 4(1)*b)*.

3 *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, chapitre 3, annexe A [*LPRPS*].

4 *Personal Information Protection Act*, L.A. 2003, chapitre P-6.5; *Personal Information Protection Act*, L.C.-B. 2003, chapitre 63; *Loi sur la protection des renseignements personnels dans le secteur privé,* L.R.Q., chapitre P-39.1. La *LPRPS* de l'Ontario a aussi été jugée essentiellement similaire à la LPRPDÉ.

pertinentes et non à la LPRPDÉ sauf dans le cas des exceptions susmentionnées. La LPRPDÉ s'applique aux activités commerciales des organisations dans toutes les autres provinces[5].

La LPRPDÉ exige que les organisations se soumettent à un ensemble d'obligations légales fondées sur les dix principes suivants : 1) responsabilité, 2) détermination des fins de la collecte des renseignements, 3) consentement, 4) limitation de la collecte, 5) limitation de l'utilisation, de la communication et de la conservation, 6) exactitude, 7) mesures de sécurité, 8) transparence, 9) accès aux renseignements personnels et 10) possibilité de porter plainte à l'égard du non-respect des principes. Le paragraphe 5(3) de la LPRPDÉ est une règle générale selon laquelle les organisations ne peuvent recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En vertu de la LPRPDÉ, toute personne peut déposer auprès de la commissaire une plainte écrite contre une organisation qui contrevient à l'une des dispositions précisées dans la Loi[6]. La commissaire peut également prendre l'initiative d'une plainte si elle a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question.

Le rôle du Commissariat à la protection de la vie privée du Canada (le Commissariat) dans le cadre de la LPRPDÉ est d'examiner les plaintes, de formuler des conclusions et d'émettre des recommandations non contraignantes, au besoin. La personne ou la commissaire peut ensuite demander à la Cour fédérale de rendre une décision relativement à l'application de la loi.

Le Commissariat a formulé des centaines de conclusions aux termes de la LPRPDÉ[7] et les tribunaux canadiens ont également rendu de nombreuses décisions. Ces conclusions et décisions, qui s'accumulent depuis les sept ans de mise en application de la LPRPDÉ, donnent un aperçu pratique des interprétations possibles de certaines des dispositions de cette loi.

Ce document fournit aux entreprises et aux personnes intéressées un aperçu des principales conclusions et décisions rendues en vertu de la LPRPDÉ jusqu'à maintenant. Dans le but de refléter l'évolution structurale des plaintes traitées en vertu de la LPRPDÉ, ce document présente les enquêtes types en fonction des thèmes suivants :

5 Les organisations des Territoires du Nord-Ouest, du Yukon et du Nunavut sont considérées comme des installations, ouvrages, entreprises ou secteurs d'activité de compétence fédérale; par conséquent, elles doivent se soumettre à la LPRPDÉ à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels dans le cadre d'activités commerciales et à l'égard des renseignements personnels sur les employés.

6 LPRPDÉ, paragraphe 11(1) : « Tout intéressé peut déposer auprès du commissaire une plainte contre une organisation qui contrevient à l'une des dispositions de la section 1 ou qui omet de mettre en œuvre une recommandation énoncée dans l'annexe 1. »

7 Les conclusions et les documents connexes peuvent être consultés sur le site Web du Commissariat à l'adresse suivante : http://www.privcom.gc.ca.

1. **Champ d'application de la Loi**

   Les enquêtes types qui ont été menées aux termes de la LPRPDÉ ont contribué à définir, entre autres, les concepts essentiels de « renseignement personnel » et d'« activité commerciale » qui aident les organisations à déterminer si la LPRPDÉ s'applique ou non dans une situation donnée.

2. **LPRPDÉ à l'étranger**

   Les enquêtes types liées à l'impartition et à d'autres activités transfrontalières ont repoussé les limites de la LPRPDÉ.

3. **Surveillance**

   Les enquêtes liées à la surveillance font partie des cas les plus litigieux découlant de l'application de la LPRPDÉ. Des enquêtes types ont donné une orientation fondamentale à la Loi dans le domaine de la surveillance pour aider les organisations à discerner la surveillance appropriée de la surveillance inappropriée.

4. **Technologies émergentes**

   Aux limites de la LPRPDÉ, plusieurs enquêtes ont permis de traiter des enjeux complexes en matière de protection de la vie privée qui découlaient de l'adoption et de l'utilisation de nouvelles technologies, y compris la biométrie et les systèmes de positionnement mondial.

5. **Atteintes à la protection des données et mesures de sécurité**

   Des cas importants d'atteinte à la protection des données ont contribué à définir les procédures et mesures de sécurité à mettre en place pour protéger les renseignements personnels.

6. **Communications négligentes et besoin de formation continue pour les employés**

   De nombreuses enquêtes ont porté sur des situations de communications négligentes ou par inadvertance de renseignements personnels. Ces enquêtes ont bien souvent souligné l'importance critique d'instaurer un processus de formation continue pour les employés, plutôt qu'une séance de formation unique.

7. **Collecte excessive de renseignements**

   Des enquêtes types dans les secteurs du commerce au détail et de l'emploi ont contribué à définir dans quelle mesure les organisations doivent limiter la quantité et la nature des renseignements personnels recueillis à différentes fins et ainsi diminuer les risques d'utilisation et de communication inappropriées de ces renseignements.

8. **Meilleur accès aux renseignements personnels**

   Plusieurs enquêtes ont permis de résoudre d'importantes préoccupations en matière de droit d'accès aux renseignements personnels, y compris des enquêtes pour lesquelles une action en justice a été intentée en parallèle et des enquêtes relatives à des frais d'accès.

9. **Fins secondaires de marketing**

   Des enquêtes types ont constitué un cadre pour déterminer la forme de consentement appropriée (consentement positif ou consentement négatif) et pour cerner les enjeux de consentement, en général dans le contexte des utilisations abusives et de la communication inappropriée des renseignements personnels à des fins secondaires de marketing.

Depuis la création de la LPRPDÉ il y a sept ans, le Commissariat et les tribunaux ont constitué un corpus indispensable de recommandations et de jurisprudence qui permettent maintenant aux organisations et aux personnes de mieux comprendre leurs droits et obligations en matière de protection de la vie privée au Canada. Les enquêtes types sont des exemples éloquents et pratiques de l'application de la LPRPDÉ; elles permettent d'orienter l'action future, notamment lorsque les organisations déploient de nouvelles technologies pour demeurer compétitives dans une économie mondiale et qu'elles se démènent pour instaurer des pratiques responsables à l'égard des renseignements personnels qui établissent un équilibre entre le droit à la vie privée et les besoins légitimes des entreprises. Les enquêtes types citées dans ce document ont été classées dans un tableau qui figure à l'annexe 1 pour en faciliter la consultation.

1. CHAMP D'APPLICATION DE LA LOI

La LPRPDÉ s'applique à la collecte, à l'utilisation et à la communication de « renseignements personnels » par une organisation dans le cadre d'une « activité commerciale »[8].

1.1 Renseignements personnels

La LPRPDÉ s'applique exclusivement à la collecte, à l'utilisation et à la communication de « renseignements personnels ». Au paragraphe 2(1) de la LPRPDÉ, la notion de « renseignement personnel » est définie en termes généraux de la façon suivante : « 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. » Bien qu'il ne soit pas toujours évident de déterminer si un renseignement est un renseignement personnel ou non, de nombreuses décisions clés rendues en vertu de la LPRPDÉ ont permis de mieux cerner cette notion. Par exemple, des enquêtes ont précisé que les types de renseignements qui suivent correspondent à la définition d'un renseignement personnel :

- les photographies[9];
- les adresses de courriel d'affaires[10];
- le numéro d'identification utilisé pour faire référence à un employé[11];

8 Les définitions de « renseignement personnel » et d'« activité commerciale » se trouvent au paragraphe 2(1) de la LPRPDÉ.

9 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 349 : Prise de photographies d'appartements de locataires sans leur consentement pour fins d'assurance – http://www.privcom.gc.ca/cf-dc/2006/349_20060824_f.asp.

10 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 297 : Courriels non sollicités pour fins de marketing – http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_f.asp.

11 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 149 : Un particulier se voit refuser l'accès à des renseignements personnels – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030409_2_f.asp.

- les adresses de protocole Internet (adresses IP)[12].

Dans un cas où un gestionnaire immobilier a pris des photographies pour montrer l'état des appartements des locataires à des fins d'assurance, la commissaire adjointe a fait clairement savoir que ces photographies, dans la mesure où elles permettent d'identifier une personne, entrent dans la définition de renseignements personnels – en d'autres mots, la personne doit être « identifiable » (des renseignements permettent de mener à son identification), pas nécessairement identifiée[13]. Dans cette affaire, la commissaire adjointe a conclu que les photographies pouvaient révéler des renseignements sur la personne qui habite le logement et sur son niveau de vie, y compris si elle aime la musique, l'art ou la cuisine. Sous chacune des photographies se trouvaient l'adresse municipale de l'immeuble et le numéro de l'appartement; ces renseignements permettent d'identifier les personnes qui habitent les appartements.

Les adresses IP peuvent constituer des renseignements personnels puisque les numéros désignent une personne identifiable, en l'occurrence, l'abonné d'un fournisseur de services Internet (FSI)[14]. Dans l'affaire *BMG Canada Inc. c. John Doe*[15], la Cour d'appel fédérale a conclu qu'un FSI ne peut volontairement communiquer l'identité des abonnés auxquels il a assigné des adresses IP particulières à des moments précis sans d'abord obtenir le consentement de ces abonnés, sauf si des exceptions légales s'appliquent.

La Cour fédérale s'est aussi penchée sur le concept d'identification potentielle dans l'affaire *Gordon c. le ministre de la Santé du Canada et la commissaire à la protection de la vie privée*[16]. Pour analyser ce qui constitue un renseignement qui permettrait d'identifier une personne, la Cour a adopté le critère juridique suivant, proposé par le Commissariat :

> [Un] renseignement concerne un individu identifiable lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que

12 Résumés de conclusions d'enquête en vertu de la LPRPDÉ nº 25 : Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web – http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_f.asp; nº 315 : Mesures de sécurité d'une société Internet et traitement d'une demande d'accès à l'information et d'une plainte relative à la protection des renseignements personnels mis en doute – http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_f.asp, et nº 319 : Mesures anti-pourriel du FSI contestées – http://www.privcom.gc.ca/cf-dc/2005/319_20051103_f.asp. Les ordinateurs communiquent entre eux sur Internet ou sur d'autres réseaux à l'aide des adresses IP. Chaque ordinateur se voit attribuer une adresse IP lorsqu'il se connecte à Internet. Le fait de connaître l'adresse utilisée par un ordinateur à un moment précis permet généralement à une organisation, avec l'aide du fournisseur de service Internet (FSI), d'identifier l'abonné qui était en ligne à ce moment précis.

13 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 349, voir la note 9 plus haut.

14 Voir les cas et le texte d'accompagnement dans la note 12 présentée plus haut.

15 *BMG Canada Inc. c. John Doe* (C.A.F.), 2005 CAF 193 (CanLII), paragraphe 37 – http://www.canlii.org/fr/ca/caf/doc/2005/2005caf193/2005caf193.html.

16 *Gordon c. Canada (Ministre de la Santé)*, 2008 CF 258 (CanLII) – http://www.canlii.org/en/ca/fct/doc/2008/2008fc258/2008fc258.html (texte en anglais seulement). Cette affaire découle de l'application de la *Loi sur la protection des renseignements personnels* (L.R.C., 1985, ch. P-21) et de la *Loi sur l'accès à l'information* (L.R., 1985, ch. A-1).

> ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles[17].

En se basant sur la preuve dans cette affaire, la Cour était d'accord avec le refus de Santé Canada de donner accès au champ de données de la province dans la base de données du Système canadien d'information sur les effets indésirables des médicaments (CADRIS). La Cour a conclu que le champ de la province combiné aux champs de données déjà divulgués et à d'autres renseignements accessibles au public (comme les notices nécrologiques) pouvait accroître considérablement la possibilité qu'une personne soit identifiée[18]. Cette situation est particulièrement vraie pour les rapports concernant une seule personne ou presque, dans les provinces et territoires plus petits.

Un autre enjeu important qui a été soulevé relativement aux « renseignements personnels » est la différence entre un renseignement « concernant » une personne et un renseignement qui n'est qu'un « produit du travail ». Dans une conclusion antérieure, l'ancien commissaire à la protection de la vie privée avait estimé que les ordonnances des médecins étaient un produit de leur travail et non pas des renseignements personnels sur eux[19]. Depuis cette conclusion, le Commissariat a adopté une approche plus globale et contextuelle. Par exemple, dans d'autres contextes, les statistiques sur les ventes des agents de télémarketing[20] et le nombre de maisons vendues dans une année par des courtiers immobiliers[21] ont été considérés comme des renseignements personnels devant faire l'objet d'une protection raisonnable en vertu de la LPRPDÉ. Le fait que des données soient produites sur un lieu de travail ne signifie pas nécessairement qu'elles ne constituent pas des renseignements personnels devant être protégés. D'autres facteurs contextuels, comme la façon dont ces données sont produites et à quelles fins elles le sont, ainsi que la manière de les utiliser, les pratiques de l'industrie, etc., doivent également éclairer l'analyse.

Dans l'affaire *Wyndowe c. Rousseau et la commissaire à la protection de la vie privée*[22], la Cour d'appel fédérale a refusé de voir dans la définition de renseignement personnel de la LPRPDÉ une exemption implicite relative au produit du travail. La Cour a conclu que les notes prises par un médecin au cours de l'examen médical indépendant (EMI) d'une personne assurée, pour le compte et aux frais d'une société d'assurances, ne sont pas des produits du travail, mais plutôt des renseignements personnels sur la personne examinée

17 *Ibid*., paragraphe 34.

18 *Ibid*., paragraphe 43.

19 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 14 : Vente de renseignements sur les habitudes de prescription des médecins – http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010921_f.asp; résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 15 : Le commissaire à la protection de la vie privée rend publiques ses conclusions sur les habitudes de prescription des médecins – http://www.privcom.gc.ca/media/an/wn_011002_f.asp.

20 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 220 : Une télévendeuse refuse que son rendement soit communiqué par son employeur à d'autres employés – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_f.asp.

21 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 303 : Un courtier immobilier publie dans une brochure publicitaire le nom des cinq meilleurs vendeurs d'une ville – http://www.privcom.gc.ca/cf-dc/2005/303_20050531_f.asp.

22 *Wyndowe c. Rousseau*, 2008 CAF 39 (CanLII) – http://www.canlii.org/en/ca/fca/doc/2008/2008fca39/2008fca39.html (texte en anglais seulement).

et sur le médecin procédant à l'EMI. Pour déterminer quelle partie des notes peut être communiquée, il faut parvenir à un équilibre en considérant les intérêts privés de la personne et ceux du médecin ainsi que l'intérêt public associé à la communication et à la non-communication[23].

1.2 Activité commerciale

Le paragraphe 2(1) de la LPRPDÉ définit une « activité commerciale » comme « toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature », y compris, expressément, « la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds. »

Plusieurs enquêtes types abordent la signification d'« activité commerciale », par exemple :

- la commissaire adjointe a conclu qu'une garderie exerçait des activités commerciales puisqu'elle réclamait le paiement des services de garde, malgré le fait qu'il s'agissait d'un organisme sans but lucratif[24];

- la commissaire adjointe a conclu que les cabinets d'avocats effectuaient des activités commerciales lorsqu'ils demandaient des rapports de solvabilité sur des parties adverses potentielles alors qu'ils représentaient des clients – un service professionnel pour lequel les cabinets étaient évidemment rémunérés[25];

- la Cour supérieure de justice de l'Ontario a jugé qu'un statut d'organisme sans but lucratif n'est pas déterminant pour décider si la collecte, l'utilisation ou la communication de renseignements personnels est effectuée dans le cadre d'une activité commerciale ou non pour une situation donnée[26];

23 La Cour d'appel fédérale a adopté une démarche similaire à celle qu'elle avait déjà adoptée pour une plainte découlant de l'application de la *Loi sur l'accès à l'information*, l'affaire *Canada (Commissaire à l'information) c. Canada (Ministre de la Citoyenneté et de l'Immigration)*, 2002 CF 950, 2002 CAF 270.

24 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 309 : Une garderie refuse à un père l'accès à des renseignements personnels qui le concernent – http://www.privcom.gc.ca/cf-dc/2005/309_20050418_f.asp.

25 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 340 : Des cabinets d'avocats recueillent des rapports de solvabilité sans le consentement des personnes concernées – http://www.privcom.gc.ca/cf-dc/2006/340_20060502_f.asp.

26 *Rodgers c. Calvert*, 2004 ON C.S. 22082 (CanLII), paragraphe 51. Même si la Cour a tranché qu'un statut d'organisme sans but lucratif n'est pas déterminant pour décider si la collecte, l'utilisation ou la communication de renseignements personnels est effectuée dans le cadre d'une activité commerciale ou non, la Cour a finalement statué que, dans cette affaire, l'organisation n'effectuait pas une activité commerciale en percevant des droits d'adhésion, car il doit y avoir plus qu'un simple échange de services pour qu'une transaction soit considérée comme commerciale.

- la Cour d'appel fédérale a jugé que lorsqu'un médecin effectue l'examen médical indépendant d'une personne assurée, pour le compte et aux frais d'une société d'assurance, aux fins d'une demande d'indemnisation, il le fait dans le cadre d'une activité commerciale[27].

Dans une affaire qui comportait des allégations voulant que le comité responsable des bourses d'études d'une école privée ait communiqué de façon inappropriée à de tierces parties des renseignements financiers sur le demandeur d'une bourse, la commissaire adjointe a pris en considération les deux points suivants pour déterminer si une activité sans but lucratif (dans ce cas-ci, l'enseignement) pouvait entrer dans la définition d'une activité commerciale :

1. Quelle est l'activité principale de l'établissement? Est-ce que les services d'éducation qu'offre l'établissement constituent ses activités principales? Dans l'affirmative, on doit présumer que ces activités ne revêtent pas un « aspect commercial ».

2. La présomption selon laquelle les activités d'un établissement scolaire ne revêtent pas d'aspect commercial est infirmée si l'un des objectifs de l'établissement est de procurer un profit aux propriétaires de l'établissement[28].

En fonction de ces deux critères, la commissaire adjointe a conclu que l'organisation en cause était une école privée dont l'activité principale était l'enseignement et que rien ne permettait de croire que l'établissement avait pour but de procurer un profit à ses propriétaires; tout soutenait l'affirmation de l'établissement selon laquelle il s'agissait d'un organisme caritatif sans but lucratif. Par conséquent, l'école était en mesure de confirmer la présomption selon laquelle elle menait des activités non commerciales.

27 *Wyndowe c. Rousseau*, voir la note 22 plus haut.

28 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 345 : Une école privée non assujettie à la LPRPDÉ – http://www.privcom.gc.ca/cf-dc/2006/345_20060705_f.asp. Le Commissariat a publié une fiche d'information sur l'application de la LPRPDÉ au secteur des municipalités, des universités, des écoles et des hôpitaux. On peut la consulter à l'adresse suivante : http://www.privcom.gc.ca/fs-fi/02_05_d_25_f.asp.

2. LPRPDÉ À L'ÉTRANGER

Les activités transfrontalières ont suscité d'importantes inquiétudes concernant la protection de la vie privée au Canada, particulièrement en ce qui a trait aux ententes d'impartition qui demandent l'envoi de renseignements personnels de Canadiennes et de Canadiens à des fournisseurs de services situés ou liés aux États-Unis. Les fournisseurs de services établis aux États-Unis peuvent être tenus de communiquer des renseignements personnels aux autorités américaines en vertu de la *USA PATRIOT Act*, ou d'un autre pouvoir légal, sans en aviser les personnes concernées.

Des inquiétudes similaires ont été suscitées concernant la communication de renseignements bancaires de Canadiennes et de Canadiens aux autorités américaines. Dans ce domaine, comme dans d'autres domaines délicats, les activités transfrontalières ont fait l'objet d'enquêtes clés qui ont étendu les limites de la LPRPDÉ au-delà des frontières canadiennes.

2.1 Impartition

Les organisations qui impartissent à l'étranger des tâches administratives qui demandent l'envoi de renseignements personnels à un tiers fournisseur de services doivent se conformer au principe 4.1.3 de la LPRPDÉ :

> Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

En vertu du principe 4.8 de la LPRPDÉ, les organisations doivent faire preuve de transparence à l'égard de leurs politiques et de leurs pratiques de gestion des renseignements personnels.

En 2005, les principes 4.1.3 et 4.8 étaient en jeu dans un cas sans précédent soumis au Commissariat à la protection de la vie privée[29]. Les plaintes portaient sur le fait que la CIBC avait fait parvenir à ses clients détenant une carte VISA un avis selon lequel un fournisseur de services situé aux États-Unis allait traiter et stocker les données relatives aux opérations de paiement. L'avis mentionnait que les autorités américaines pourraient avoir accès aux renseignements personnels des clients. L'entente d'impartition de la CIBC avait été approuvée par le Bureau du surintendant des institutions financières. La CIBC avait aussi un contrat avec son fournisseur de services comprenant, entre autres, des clauses relatives à la confidentialité, à la sécurité, à la surveillance, à la supervision, à la vérification, à la garde et au contrôle.

Ce cas rappelle qu'une organisation, dans une situation où elle impartit le traitement de renseignements personnels à un tiers fournisseur de services situé à l'étranger, demeure responsable en vertu du principe 4.1.3 des renseignements personnels qu'on lui a confiés. La commissaire adjointe a conclu que la CIBC avait satisfait à l'obligation de garantir, par voie contractuelle, un degré de protection comparable à ce qu'elle offre elle-même en vertu du principe 4.1.3. Malgré le fait qu'il y avait un risque que des renseignements personnels soient communiqués aux autorités américaines, la commissaire adjointe a conclu que ce risque était comparable à celui d'une communication obligatoire de ces renseignements aux autorités canadiennes en vertu de pouvoirs légaux si le fournisseur de services avait été situé au Canada.

La commissaire adjointe a précisé que la LPRPDÉ ne peut ni empêcher les organisations qui lui sont assujetties d'impartir des services à des fournisseurs de services situés à l'étranger, ni empêcher un gouvernement étranger d'accéder légalement à des renseignements personnels sous la garde des organisations établies sur son propre territoire. Toutefois, la LPRPDÉ oblige les organisations qui lui sont assujetties à être transparentes au sujet de leurs pratiques de gestion des renseignements personnels et à protéger, par voie contractuelle et dans la mesure du possible, les renseignements confiés à des tiers fournisseurs de services à l'étranger.

L'affaire CIBC démontre que les principes 4.1.3 et 4.8, lorsque combinés, exigent qu'une organisation visée, au minimum 1) soit en mesure, par voie contractuelle ou autre, de fournir un degré de protection des renseignements comparable à ce qu'elle offre elle-même, 2) informe ses clients au sujet de ses politiques et pratiques de gestion des renseignements personnels et 3) avise ses clients que leurs renseignements personnels pourront être accessibles à un gouvernement étranger ou à ses organismes en vertu de pouvoirs légaux du pays en question.

Peu après l'affaire de la CIBC, la commissaire adjointe a émis des conclusions relativement à la circulation transfrontalière de renseignements personnels entre une

29 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 313 : Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA PATRIOT Act* – http://www.privcom.gc.ca/cf-dc/2005/313_20051019_f.asp.

société mère et une filiale[30]. Dans cette affaire, la filiale canadienne d'un fournisseur de systèmes de sécurité a informé ses clients que, dans certaines circonstances, elle pourrait partager des renseignements avec sa société mère aux États-Unis. L'avis précisait qu'en cas de catastrophe qui affecterait un centre de surveillance situé au Canada, les signaux d'alarme seraient acheminés vers un autre centre qui pourrait être situé aux États-Unis. L'avis donnait aux clients la possibilité de demander que leurs renseignements ne soient pas communiqués, mais les informait que s'ils le faisaient, ils pouvaient s'attendre à une baisse de la qualité du service.

Dans des situations d'impartition où les parties sont liées, comme une filiale et sa société mère, la commissaire adjointe a conclu que même s'il n'est pas nécessaire d'établir un contrat entre les organisations affiliées, celles-ci doivent néanmoins adopter le même degré de protection des données personnelles. Dans cette affaire, les organisations avaient en place un réseau privé fermé et des mesures de protection exhaustives pour les renseignements. La commissaire adjointe a constaté que les organisations avaient fourni des degrés comparables de protection et que les clients avaient été adéquatement informés du risque que des renseignements personnels puissent être légalement communiqués à des autorités américaines.

En 2007, la commissaire adjointe a enquêté sur un troisième cas sans précédent de circulation transfrontalière des données reliée à l'impartition : l'affaire SWIFT[31]. Cette affaire concernait la communication massive de renseignements bancaires aux autorités américaines par l'intermédiaire d'un tiers fournisseur de services, en l'occurrence, la Society for Worldwide Interbank Financial Telecommunication (SWIFT), établie en Belgique.

Les banques canadiennes ont un accord contractuel avec la SWIFT selon lequel les banques envoient des renseignements financiers personnels sur des clients à la SWIFT à des fins de traitement des messages financiers internationaux, y compris des mandats.

Dans l'enquête sur la plainte contre les banques canadiennes, la commissaire adjointe a examiné attentivement les contrats passés entre les banques et la SWIFT. En se basant sur le raisonnement du cas de la CIBC, elle a estimé que les contrats et les mesures en place garantissaient un degré comparable de protection. Elle a également estimé que les banques avaient informé leurs clients de façon appropriée à propos du risque de communication obligatoire de renseignements à des autorités étrangères par des énoncés clairs dans les politiques de protection des renseignements personnels des banques. Conséquemment, la commissaire adjointe a conclu que la plainte contre les banques canadiennes était non fondée.

30 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 333 : Une entreprise canadienne communique les renseignements personnels de ses clients à la société mère située aux États-Unis – http://www.privcom.gc.ca/cf-dc/2006/333_20060511_f.asp.

31 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 365 : Responsabilité d'institutions financières canadiennes dans la communication de renseignements personnels par SWIFT aux autorités des États-Unis – http://www.privcom.gc.ca/cf-dc/2007/365_20070402_f.asp.

Dans le cadre d'une plainte indépendante contre la SWIFT déposée à l'initiative de la commissaire, cette dernière s'est penchée sur l'application de la LPRPDÉ à la SWIFT[32]. Cette importante enquête est présentée dans la section suivante, qui porte sur l'application de la LPRPDÉ aux entités étrangères.

2.2 Application de la LPRPDÉ aux entités étrangères

Dans deux décisions importantes rendues en 2007, l'application de la LPRPDÉ s'est étendue bien en dehors des frontières du Canada.

Dans l'affaire *Lawson c. Accusearch*[33], la Cour fédérale a annulé la décision rendue par la commissaire adjointe selon laquelle elle n'avait pas compétence pour faire enquête quant à une plainte contre une entité située à l'extérieur du Canada dans les circonstances particulières de cette affaire. La plainte portait sur la collecte, l'utilisation et la communication, par une société américaine, de renseignements personnels à des partenaires payants, à savoir des personnes et des clients du Canada, ainsi que d'un grand nombre d'autres pays. La plaignante, résidant au Canada, a commandé et obtenu de la part de l'entreprise une vérification de ses antécédents pour laquelle elle a payé dans le but de démontrer les pratiques de l'entreprise en ce qui a trait aux renseignements personnels et d'appuyer son argument selon lequel ces pratiques étaient inappropriées et allaient à l'encontre de la LPRPDÉ.

L'argument de la commissaire adjointe, retenu par la Cour fédérale, était que la LPRPDÉ n'était pas destinée à avoir une portée extraterritoriale : « Le législateur ne pouvait avoir l'intention que la LPRPDÉ régisse la cueillette et l'utilisation de renseignements personnels dans le monde entier ». Néanmoins, la Cour a conclu que la LPRPDÉ peut encore s'appliquer aux entités étrangères qui reçoivent ou transmettent des communications à destination et en provenance du Canada et qui recueillent et communiquent des renseignements personnels *au sujet de personnes résidant au Canada*. Dans les circonstances particulières de cette affaire, la Cour a conclu que les renseignements personnels de la plaignante devaient provenir de sources canadiennes, même si elles n'ont pas pu être identifiées[34]. Toutefois, la Cour ne s'est pas prononcée pour déterminer quels facteurs de rattachement réels et importants au Canada devront être présents dans les causes futures pour que la commissaire ait le pouvoir de mener une enquête. Le fait que l'enquête puisse être contrecarrée et inefficace en pratique, en raison du manque de collaboration de l'organisation et de la difficulté de la part de

32 Rapport de conclusions (2 avril 2007) – http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_f.asp.

33 *Lawson c. Accusearch Inc.*, 2007 CF 125 (CanLII) – http://www.canlii.org/fr/ca/cfpi/doc/2007/2007cf125/2007cf125.html; annulation de décision : « [La] commissaire à la protection de la vie privée du Canada a publié [une] lettre sur Abika.com, un courtier en données en ligne aux États-Unis qui recueille, utilise et communique les renseignements personnels des Canadiennes et des Canadiens. » (18 novembre 2005) – http://www.privcom.gc.ca/legislation/let/let_051118_f.asp

34 *Ibid.* (Au paragraphe 41, la Cour a déclaré : « Bien que la commissaire ait soutenu avec peu de conviction que rien ne prouvait l'existence d'un lien avec le Canada, cet argument ne constituait pas le fondement de sa décision. Même si le "profil psychologique" de M^me^ Lawson était inventé de toute pièce et avait été écrit aux États-Unis, une bonne partie des données devait provenir du Canada. La commissaire l'a reconnu dans sa décision quand elle a écrit : "Abika.com n'a pas répondu à notre demande d'obtention des noms de ses sources canadiennes". »)

la commissaire d'assigner un étranger à comparaître, n'empêche pas la commissaire d'affirmer sa compétence à l'égard de l'affaire dès le début. La Cour a renvoyé l'affaire à la commissaire et a ordonné à celle-ci de mener une enquête sur la plainte contre l'entreprise américaine en question, malgré les difficultés d'ordre pratique qui peuvent survenir.

Le deuxième cas concernant l'application de la LPRPDÉ aux entités étrangères est la plainte déposée par la commissaire contre la SWIFT dans le cadre de l'affaire susmentionnée[35]. Parallèlement à la plainte contre les banques canadiennes impliquées, la commissaire devait décider si la LPRPDÉ s'appliquait également aux activités de la SWIFT, l'impartiteur établi en Belgique qui recueillait des données financières sur des clients de banques canadiennes à des fins de traitement et les communiquait aux autorités américaines. Pour vérifier si la SWIFT devait se soumettre à la LPRPDÉ, la commissaire a examiné les liens réels et importants ci-dessous entre la SWIFT et le Canada :

- la SWIFT recueillait des renseignements personnels auprès des banques canadiennes et leur en communiquait;
- la SWIFT facturait des frais aux banques canadiennes pour ses services;
- 14 des actionnaires de la SWIFT étaient Canadiens;
- un des directeurs de la SWIFT provenait d'une banque canadienne;
- la plupart des communications transfrontalières de renseignements personnels qui provenaient de banques canadiennes ou qui leur étaient destinées étaient transmises par la SWIFT;
- la SWIFT faisait partie intégrante du système financier canadien.

D'après ces facteurs de rattachement réels et importants, la commissaire a conclu que la SWIFT se livrait à une activité commerciale au Canada et qu'elle devait, par conséquent, assumer des responsabilités organisationnelles conformément à la LPRPDÉ.

Sur la question de fond de savoir si la SWIFT a effectivement enfreint la LPRPDÉ, la commissaire a conclu que l'alinéa 7(3)*c)* autorisait la SWIFT à communiquer les renseignements, comme elle l'a fait, en réponse à une assignation à comparaître valide émise aux États-Unis. Selon la commissaire, l'alinéa 7(3)*c)* de la LPRPDÉ autorise les organisations à répondre aux assignations, mandats ou ordonnances des autorités et des tribunaux non seulement canadiens, mais également étrangers. La commissaire a précisé qu'il serait « peu réaliste, voire impossible » de demander aux multinationales de ne pas tenir compte des lois des autres pays où elles exercent leurs activités en plus de respecter

35 Rapport de conclusions, voir la note 31 plus haut.

celles du Canada. Ne pas tenir compte de la loi d'un autre pays équivaudrait à enfreindre la souveraineté de cette nation[36]. Les organisations qui communiquent en toute légitimité des renseignements personnels à l'extérieur du Canada[37] devraient donc être autorisées, conformément à l'alinéa 7(3)*c*), à communiquer ces renseignements aux autorités étrangères en vertu du pouvoir légal de ces autres pays où elles exercent leurs activités.

36 *Ibid.* – cf. paragraphe 48.

37 Voir la discussion de la section 2.1 de ce document.

3. SURVEILLANCE

Les cas de surveillance font partie des cas les plus litigieux découlant de l'application de la LPRPDÉ. Ils servent de référence pour la définition de fins acceptables selon le paragraphe 5(3) de la LPRPDÉ.

Le paragraphe 5(3) de la LPRPDÉ permet aux organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels « à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Il s'agit d'une exigence très importante de la Loi. On ne peut s'y soustraire par consentement et elle s'applique malgré toutes les exceptions relatives au consentement qui pourraient aussi être admises.

Par exemple, selon l'alinéa 7(1)*b*) de la LPRPDÉ, une organisation peut recueillir des renseignements personnels sans le consentement de l'intéressé dans le cas suivant :

> il est raisonnable de s'attendre à ce que la collecte effectuée au su ou avec le consentement de l'intéressé puisse compromettre l'exactitude du renseignement ou l'accès à celui-ci, et la collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial.

Les organisations se fondent souvent sur cette exception lorsqu'elles utilisent la surveillance pour combattre la criminalité ou enquêter sur l'inconduite des employés. Toutefois, même si les organisations peuvent démontrer que leur utilisation de la surveillance vidéo est visée par cette exception relative au consentement, elles doivent être en mesure de démontrer que la surveillance vidéo est utilisée sans consentement de l'intéressé à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances aux termes du paragraphe 5(3).

3.1 Surveillance à des fins de sécurité

L'arrêt faisant autorité en matière de surveillance en vertu de la LPRPDÉ est *Eastmond c. Canadien Pacifique Ltée*[38]. Il a été cité avec approbation dans un grand nombre de cas subséquents.

Dans l'affaire *Eastmond*, des employés ont déposé une plainte en vertu de la LPRPDÉ puisque que leur employeur, Canadien Pacifique Limitée (CP), avait installé six caméras vidéo dans un triage. Les caméras étaient fixes, sans panoramique horizontal ni fonction de zoom. Le CP conservait les enregistrements des caméras pour une période limitée dans une armoire verrouillée, et ne visionnait les enregistrements que si un incident signalé à la direction était susceptible d'avoir été capté par les caméras. Sinon, les enregistrements étaient effacés.

L'entreprise a donné trois raisons d'installer les six caméras : 1) prévenir le vol, le vandalisme et l'intrusion, 2) améliorer la sécurité du personnel et 3) collaborer à l'enquête sur tout incident signalé survenu sur les lieux.

Pour évaluer si une personne raisonnable estimerait les fins du CP acceptables dans les circonstances, le commissaire a constitué et appliqué un critère en quatre points en vertu du paragraphe 5(3) de la LPRPDÉ :

(i) **Est-il possible de faire la preuve que la surveillance et l'enregistrement au moyen de caméras sont nécessaires** pour répondre à un besoin particulier?

(ii) La **surveillance et l'enregistrement au moyen de caméras** sont-ils susceptibles d'être efficaces pour répondre à ce besoin?

(iii) La perte de vie privée est-elle proportionnelle à l'avantage obtenu?

(iv) Existe-t-il un moyen portant moins atteinte à la vie privée qui pourrait permettre d'atteindre le même but?

Lors de l'application du critère dans l'affaire *Eastmond*, le commissaire a conclu que les fins du CP n'étaient pas acceptables parce que l'entreprise n'a pas réussi à démontrer l'existence d'un problème réel nécessitant plus d'attention. Le commissaire a ajouté que, même si le CP avait prouvé l'existence d'un problème, il ne croyait pas que les caméras permettraient de s'y attaquer efficacement. Une demande de révision à la Cour fédérale a été présentée en vertu de l'article 14 de la LPRPDÉ.

38 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 114 : Un employé s'oppose à l'utilisation de caméras vidéo numériques de surveillance par la compagnie –http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_f.asp; *Eastmond c. Canadien Pacifique Ltée*, 2004 CF 852 (CanLII), 16 Admin. L.R. (4e) 275 –http://www.canlii.org/fr/ca/cfpi/doc/2004/2004cf852/2004cf852.html.

Bien que la Cour fédérale ait affirmé que le critère en quatre points pourrait ne pas s'appliquer à tous les autres contextes, la Cour a entrepris d'appliquer ce critère en fonction des nouveaux éléments de preuve présentés à l'audition *de novo* et a obtenu des résultats différents. Cette analyse est cruciale pour toute organisation qui songe à adopter des mesures de surveillance.

Au premier élément du critère, la Cour a conclu que le CP avait établi la nécessité légitime de faire installer les caméras en se fondant sur les incidents survenus dans le triage et dans d'autres cours. L'historique des incidents, ainsi que l'effet dissuasif potentiel des caméras pour prévenir de futurs incidents, était suffisant pour montrer qu'il s'agissait d'un réel problème auquel il fallait trouver une solution.

Au deuxième critère, en se fondant sur la preuve qu'aucun incident n'avait été signalé dans le triage depuis l'installation des caméras, la Cour a déclaré que les caméras répondaient probablement au besoin de l'entreprise. La Cour s'est également fiée aux éléments de preuve démontrant l'efficacité des mesures de surveillance similaires adoptées dans les autres cours du CP.

Au troisième critère, la Cour a conclu que la perte de vie privée était proportionnelle à l'avantage obtenu. Dans cette affaire, les avantages en matière de sécurité obtenus grâce aux caméras avaient été établis. La perte de vie privée était minime parce que 1) l'enregistrement avait lieu dans un endroit où les personnes avaient de faibles attentes quant au respect de la vie privée et 2) le CP avait pris divers moyens pour s'assurer que la violation de la vie privée reste aussi minime que nécessaire pour parvenir à ses fins, à savoir :

- le CP a installé des panneaux d'avertissement indiquant que des caméras avaient été installées;
- les caméras ne surveillaient pas les employés, puisqu'elles étaient fixes;
- les caméras ne ciblaient pas les employés en particulier – elles captaient aussi des images d'entrepreneurs, de visiteurs, de fournisseurs et d'intrus;
- les caméras ne servaient pas à mesurer le rendement des employés;
- les enregistrements étaient conservés dans un endroit sûr; seuls la police et les gestionnaires du CP les visionnaient, et seulement lorsqu'un incident était signalé.

Pour terminer, lors de l'évaluation à savoir s'il existait un moyen qui porterait moins atteinte à la vie privée et permettrait d'arriver au même but de façon économique, la Cour a accepté les éléments de preuve du CP selon lesquels il avait envisagé et rejeté d'autres mesures, y compris des clôtures et des gardes de sécurité.

La Cour a conclu qu'une personne raisonnable considérerait les mesures du CP acceptables dans les circonstances.

À la suite de l'affaire *Eastmond* et de nombreux autres cas pertinents concernant l'utilisation de la surveillance vidéo, le Commissariat a élaboré des lignes directrices pour les organisations qui songent à utiliser la surveillance vidéo dans leurs installations.

Lignes directrices du CPVP sur la surveillance vidéo au moyen d'appareils non dissimulés dans le secteur privé (mars 2008) http://www.privcom.gc.ca/information/guide/2008/gl_vs_080306_f.asp

1. Vous demander si un moyen portant moins atteinte à la vie privée que la surveillance vidéo pourrait répondre à vos besoins.
2. Déterminer les fins opérationnelles de la surveillance vidéo et limiter son utilisation à ces fins.
3. Élaborer une politique sur l'utilisation de la surveillance vidéo.
4. Limiter autant que possible l'utilisation et la portée visuelle des caméras.
5. Informer le public que l'on effectue une surveillance vidéo.
6. Entreposer toutes les images enregistrées dans un lieu sûr et d'accès restreint, et les détruire lorsqu'elles n'ont plus d'utilité opérationnelle.
7. Se préparer à répondre aux questions du public. Les personnes ont le droit de savoir qui les observe et pourquoi, quelle information est recueillie, et ce que l'on fait des images enregistrées.
8. Offrir aux personnes l'accès aux renseignements les concernant, y compris les images vidéo.
9. Sensibiliser les opérateurs de caméra à l'obligation de protéger la vie privée des gens.
10. Évaluer périodiquement la nécessité d'utiliser la surveillance vidéo.

Remarque : *Les présentes lignes directrices s'appliquent à la surveillance vidéo du public par des organisations du secteur privé au moyen d'appareils non dissimulés, placés dans des lieux publics. Elles ne s'appliquent pas à la surveillance vidéo au moyen d'appareils dissimulés, comme celle menée par des détectives privés pour le compte de compagnies d'assurances, ni à la surveillance des employés.*

3.2 Surveillance des employés

Dans une autre enquête ayant établi un précédent, une organisation a utilisé des caméras – qui servent normalement à suivre le mouvement des trains et à informer les membres d'équipage de l'emplacement des trains – pour établir si des employés avaient quitté les lieux pendant les heures normales de travail[39]. L'organisation a pris des mesures disciplinaires contre les fautifs. Toutefois, elle n'a présenté aucune preuve attestant que les absences non autorisées du lieu de travail constituaient un problème persistant chez les plaignants ou chez d'autres employés. De plus, elle n'a produit aucune preuve à l'égard d'autres efforts qu'elle aurait déployés pour faire échec au problème des absences non autorisées.

La commissaire adjointe a conclu qu'une personne raisonnable ne jugerait pas acceptable, dans les circonstances, l'utilisation de caméras à des fins disciplinaires. Cette utilisation contrevenait donc au paragraphe 5(3) de la LPRPDÉ. La commissaire a précisé que, s'il

39 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 265 : Caméras vidéo au travail –http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_f.asp.

existe une méthode moins envahissante permettant d'obtenir le même résultat, celle-ci devrait être le premier recours, même dans les cas où l'organisation invoque l'exception en vertu de l'alinéa 7(1)*b*) qui prévoit la collecte de renseignements sans le consentement de l'intéressé.

D'autres enquêtes types liées à des situations de surveillance en milieu de travail ont permis d'établir les principes suivants :

- La surveillance vidéo continuelle et sans discrimination n'est pas acceptable si les caméras ciblent les aires de travail des employés avec le but exprès, entre autres, de gérer la productivité des employés, en particulier lorsque des mesures moins envahissantes existent. La commissaire adjointe a précisé que le « coût de la dignité humaine [doit faire] partie intégrante de l'équation » pour trouver un bon équilibre entre la surveillance et le droit à la vie privée[40];

- Les caméras sont acceptables si l'organisation a clairement fait la preuve qu'elles sont utilisées pour des raisons légitimes de sécurité, si les caméras ciblent les aires d'accès aux installations et non les aires de travail, si les enregistrements sont conservés pour une période limitée puis effacés, et si l'organisation informe les employés des justifications de leur utilisation et des fins pour lesquelles les renseignements personnels les concernant sont réunis[41];

- L'utilisation de caméras en milieu de travail n'est pas acceptable s'il n'est pas possible de faire la preuve que cette mesure est nécessaire pour répondre à un besoin opérationnel ou si elle n'est pas susceptible d'être efficace pour répondre à ce besoin, par exemple lorsque des caméras ne donnent pas une image assez précise pour assurer la sécurité du produit – motif invoqué par l'entreprise – et qu'il existe d'autres moyens plus efficaces et moins envahissants d'atteindre le même objectif;[42]

- L'embauche d'un enquêteur pour exercer une surveillance est acceptable en vertu de l'alinéa 7(1)*b*) si l'organisation a un motif raisonnable et probable de croire qu'un employé

40 Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ nº 279 : La surveillance des employés au travail – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_f.asp.

41 Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ nº 264 : Caméras vidéo et cartes magnétiques au travail – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_f.asp.

42 Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ nº 290 : Les caméras de surveillance contestées dans un établissement de transformation de produits alimentaires - http://www.privcom.gc.ca/cf-dc/2005/290_050127_f.asp. Fait également pertinent, les caméras ne donnaient pas une image précise des produits alimentaires transformés.

> enfreint son contrat de travail en faisant une déclaration trompeuse sur son état de santé et si elle a employé sans succès d'autres méthodes qui portent moins atteinte à la vie privée[43].

Une autre enquête type qui est liée à la surveillance au moyen d'un système de localisation (GPS) est présentée dans la section suivante du document, qui porte sur les technologies émergentes.

43 Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ nº 269 : L'employeur embauche un enquêteur privé pour exercer une surveillance vidéo d'un employé – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040423_f.asp.

4. TECHNOLOGIES ÉMERGENTES

La LPRPDÉ a été adoptée, entre autres, pour réagir aux menaces à la vie privée de nature technologique, comme l'énonce clairement l'article 3 : « La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels […] ».

La LPRPDÉ ne renferme pas de dispositions qui portent sur des types particuliers de technologies. Elle est un instrument réglementaire général qui couvre tous les secteurs et toutes les activités indépendamment de la technologie utilisée. Néanmoins, il n'est pas surprenant que des menaces à la vie privée apparaissent régulièrement relativement à l'utilisation de technologies émergentes.

La technologie sous-tend un grand nombre d'activités potentiellement intrusives. Aux limites de la LPRPDÉ, plusieurs enquêtes importantes ont permis de traiter des enjeux en matière de protection de la vie privée qui découlaient de l'utilisation de nouvelles technologies[44], y compris la biométrie et les systèmes mondiaux de localisation (GPS).

4.1 Biométrie

Dans le cadre d'une enquête type liée à la technologie, la commissaire adjointe a examiné une plainte déposée par des employés parce que leur employeur les obligeait à fournir des données biométriques les concernant, en l'occurrence leur « empreinte vocale », dans le but d'authentifier les utilisateurs du réseau interne et d'en sécuriser l'accès à distance. Les employés avaient besoin d'accéder au réseau pour entrer des données liées au travail et déclarer des absences[45]. L'enjeu principal de cette enquête était de déterminer si la technologie vocale – appelée e.Speak – était utilisée « à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances » aux termes du paragraphe 5(3) de la LPRPDÉ.

44 La notion de technologie est également incluse dans la définition de « renseignements personnels ». Voir la partie concernant les adresses IP et les activités en ligne à la section 1.1 de ce document.

45 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 281 – Une organisation utilise la biométrie à des fins d'authentification – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_f.asp.

L'organisation avait choisi d'utiliser un système de reconnaissance vocale parce que les employés sur le terrain emportaient des téléphones sur leurs lieux de travail, et que ce système constituait un moyen efficace d'accéder à distance au réseau interne de l'organisation. Selon l'organisation, un système de reconnaissance vocale était préférable à un système de mots de passe traditionnel puisqu'il était plus rentable et qu'il offrait un niveau de sécurité plus élevé en ce qui concerne les données sur les clients saisies par les employés. L'organisation avait établi un certain nombre de contrôles de sécurité rigoureux pour accéder à la base de données dans laquelle étaient sauvegardées les empreintes vocales. Seul un nombre restreint de personnes pouvait y accéder et pour des utilisations précises seulement. L'empreinte vocale d'un employé était éliminée dans le mois suivant la date à partir de laquelle il n'était plus autorisé à utiliser le système.

À la lumière de ces facteurs, la commissaire adjointe était d'avis qu'une personne raisonnable estimerait que les fins de l'organisation étaient acceptables, conformément au paragraphe 5(3), d'autant plus que les empreintes vocales ne sont pas vraiment des renseignements personnels sensibles et que le système e.Speak augmente la sécurité des renseignements personnels des clients dans le cas particulier de cette affaire. Puisque les employés devaient fournir consciemment un échantillon de leur voix, la commissaire adjointe a reconnu que l'organisation avait obtenu le consentement implicite des personnes dont l'empreinte vocale avait été recueillie. Par contre, cette conclusion de consentement implicite n'a pas été émise sans difficulté, surtout si l'on considère la réalité du milieu du travail et l'inégalité du pouvoir de négociation entre l'employeur et l'employé.

En vertu de l'article 14 de la LPRPDÉ, les employés ont demandé une audience à la Cour fédérale[46] et ont ultérieurement interjeté appel à la Cour d'appel fédérale[47]. Les deux cours ont reconnu que l'organisation avait adopté le système e.Speak à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances, selon l'analyse des éléments suivants :

- le degré de sensibilité des empreintes vocales comme renseignements personnels;
- les mesures de sécurité mises en œuvre par TELUS;
- les intérêts commerciaux légitimes de TELUS que vise la collecte d'empreintes vocales;
- l'efficacité des empreintes vocales dans l'atteinte de ces objectifs;
- le caractère raisonnable de la collecte d'empreintes vocales par rapport à d'autres méthodes permettant d'atteindre le même niveau de sécurité à des coûts et avec des avantages opérationnels comparables;

46 *Turner c. TELUS Communications Inc.*, 2005 CF 1601 (CanLII).

47 *Wansink c. TELUS Communications Inc.* (C.A.F.), 2007 CAF 21 (CanLII).

- la proportionnalité de l'atteinte à la vie privée des employés par rapport au coût et aux avantages opérationnels compte tenu des mesures de sécurité fournies par TELUS.

En ce qui a trait au consentement, la Cour d'appel fédérale a confirmé que toutes les exceptions permettant la collecte, l'utilisation et la communication de renseignements personnels sans le consentement de l'intéressé sont exhaustivement énoncées à l'article 7 de la LPRPDÉ et qu'aucune ne s'appliquait dans les circonstances. Toutefois, la Cour a déclaré que la conception même du système e.Speak permettait de s'assurer que le consentement des personnes avait été fourni avant la collecte des échantillons de leur voix. Sans la participation effective des employés, l'entreprise ne pouvait pas créer les empreintes vocales et les entrer dans le système. Fait à noter, la Cour d'appel n'a pas tranché la question de savoir si les menaces de mesures disciplinaires alléguées contre les employés qui ont refusé de donner leur consentement auraient pu invalider leur consentement explicite aux termes de la Loi[48].

4.2 GPS

Dans le cadre d'une autre enquête type liée à la technologie, la commissaire adjointe a examiné une plainte qui avait été déposée par des employés dont l'employeur installait un GPS dans les véhicules de travail. Ce système servait à recueillir de l'information sur leurs déplacements quotidiens durant les heures de travail, notamment le temps où ils démarraient et arrêtaient les véhicules, la vitesse des véhicules, leur emplacement, leur kilométrage et l'endroit où ils se garaient en dehors du quart de travail[49]. Les conducteurs ne pouvaient pas mettre le GPS hors tension. La commissaire adjointe a jugé que les données sur les conducteurs recueillies au moyen du GPS étaient des « renseignements personnels », même si l'identité des conducteurs n'était pas toujours révélée aux employés qui accédaient aux données du GPS. Tout comme pour l'enquête sur la biométrie susmentionnée et pour les autres enquêtes présentées dans la section sur la surveillance de ce document, l'enjeu principal consistait à savoir si l'organisation utilisait le GPS à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

L'organisation a invoqué les raisons suivantes pour justifier la collecte et l'utilisation des renseignements personnels recueillis au moyen du GPS :

- *Gestion de la productivité de la main-d'œuvre* – Selon l'organisation, le GPS servait à localiser les employés, à leur assigner une tâche et à les diriger vers leurs lieux d'affectation. L'information sur le début et la fin des périodes pendant lesquelles les véhicules étaient en service,

48 *Ibid.*, paragraphe 28. La Cour a fait savoir, dans une remarque incidente au paragraphe 29, que si TELUS avait fait des menaces de mesures disciplinaires telles que la suspension ou le congédiement lorsque les employés refusaient de se prêter à la collecte d'empreintes vocales, ces menaces auraient alors invalidé le consentement.

49 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 351 – Examen de l'utilisation des renseignements personnels recueillis au moyen d'un système mondial de localisation – http://www.privcom.gc.ca/cf-dc/2006/351_20061109_f.asp.

ainsi que celle sur l'endroit où les véhicules se trouvaient, servait, au besoin, à des fins de planification de la capacité, d'analyse de la productivité et de gestion du rendement;

- *Sécurité et perfectionnement* – Selon l'organisation, le GPS servait à déterminer si un véhicule était demeuré stationnaire pendant un laps de temps anormalement long, laissant suggérer que la sécurité d'un employé était compromise. En outre, l'information recueillie au moyen du GPS pouvait servir à déterminer les employés qui pouvaient bénéficier d'une formation sur la conduite préventive et prudente ou d'une aide individuelle à la lumière des statistiques sur la vitesse;

- *Protection et gestion des biens* – L'information recueillie au moyen du GPS relativement à l'emplacement d'un véhicule pouvait servir à repérer le véhicule dans l'éventualité où il aurait été volé ou abandonné ou s'il devait être soumis à une vérification. L'organisation a soutenu qu'elle avait réduit ses coûts depuis l'installation du système; elle avait notamment enregistré une baisse de consommation d'essence et du kilométrage parcouru par ses véhicules.

La commissaire adjointe a effectué une analyse détaillée des raisons invoquées par l'organisation et a approuvé la plupart d'entre elles dans les circonstances de cette affaire :

1) Pour ce qui est d'utiliser le GPS dans le but d'améliorer la répartition, la commissaire adjointe était d'avis que l'atteinte à la vie privée était proportionnelle aux avantages tirés et qu'il n'y avait aucune façon moins envahissante de réaliser ce but;

2) La commissaire adjointe a accepté l'utilisation du GPS à des fins de sécurité. Elle a noté que le système était utilisé de façon suffisamment efficace pour assurer la sécurité des employés et du public, et que l'atteinte à la vie privée était proportionnelle aux avantages tirés;

3) La commissaire adjointe a convenu que la protection et la gestion des biens constituaient des raisons appropriées en vertu du paragraphe 5(3) pour lesquelles il y avait consentement implicite;

4) Cependant, la commissaire adjointe s'est dite préoccupée par la possibilité d'utiliser un système GPS pour évaluer le rendement des employés à la lumière des conclusions tirées au moyen des données recueillies par le GPS. Si l'organisation envisage de se servir du GPS à des fins de gestion des employés dans des « circonstances limitées, exceptionnelles et bien définies », elle doit en informer clairement ses employés et élaborer une politique décrivant dans ses grandes lignes un processus approprié pour les avertissements et le contrôle progressif. Les

données recueillies au moyen du GPS ne devraient pas être couramment utilisées dans le contexte de la gestion des employés. La commissaire adjointe a souligné l'importance de prendre en compte la dignité des employés pour concilier le droit des personnes à la vie privée et les besoins des organisations.

L'organisation a donc établi une politique sur l'utilisation des données recueillies au moyen du GPS à des fins de gestion du rendement qui énonce clairement les conditions et explique les circonstances exceptionnelles où ces données pourraient aider à examiner un enjeu de productivité. Elle s'est également engagée à former tous ses gestionnaires afin de s'assurer qu'ils utilisent le GPS de façon appropriée et non pour surveiller continuellement l'emplacement des employés. L'organisation s'est également engagée à informer ses employés au sujet du système et de ses utilisations, ce qui doit normalement être fait *avant* l'exécution d'un programme particulier, et non après. Par conséquent, la commissaire adjointe s'est dite convaincue que l'utilisation du GPS à des fins de gestion du rendement est appropriée dans des circonstances limitées, exceptionnelles et bien définies, conformément à la politique de l'organisation et au paragraphe 5(3).

5. ATTEINTES À LA PROTECTION DES DONNÉES ET MESURES DE SÉCURITÉ

Les cas importants d'atteinte à la protection des données sont en augmentation à l'échelle planétaire. Il ne se passe pas une journée sans qu'on entende parler d'un ordinateur portable égaré qui contenait des renseignements personnels ou d'une atteinte à la protection des données qui a permis la divulgation de renseignements personnels sur Internet.

En vertu du principe 4.7 de la LPRPDÉ, les organisations doivent protéger les renseignements personnels au moyen de mesures de sécurité correspondant au degré de sensibilité, à la quantité, à la répartition et au format de ces renseignements. Plus le degré de sensibilité des renseignements est élevé, plus les mesures de sécurité doivent être rigoureuses. Le principe 4.7.1 précise que ces mesures doivent « protéger les renseignements personnels contre la perte ou le vol, ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. »

Le principe 4.7.3 recommande aux organisations d'inclure les méthodes de protection suivantes dans les mesures de sécurité :

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;

b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif;

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

Au Canada, de nombreuses enquêtes ont contribué à définir la nature et le degré des mesures de sécurité que les organisations doivent mettre en place pour protéger les renseignements personnels en vertu de la LPRPDÉ. Ces enquêtes sont présentées dans cette section.

5.1 Atteintes à la protection des données

En 2007, même si des enquêtes précédentes avaient établi des lignes directrices pour l'application de la Loi, l'enquête visant TJX, exploitant les magasins Winners et HomeSense, allait établir un précédent. Cette enquête propose une analyse beaucoup plus détaillée des exigences en matière de sécurité dans le contexte actuel[50].

Vers la fin de 2006, TJX a découvert un logiciel suspect dans un de ses systèmes informatiques et a appris qu'un intrus avait accédé à des renseignements personnels de ses clients, y compris aux numéros et dates d'expiration de cartes de crédit, aux noms, adresses et numéros de téléphone, aux données sur les permis de conduire et aux numéros d'identification provinciaux.

Au début de 2007, TJX a informé le Commissariat que ses systèmes informatiques avaient fait l'objet d'une intrusion et que les renseignements personnels associés à environ 45 millions de cartes de paiement, y compris des cartes canadiennes, pouvaient être touchés. TJX supposait que l'intrus avait accédé à ses systèmes au moyen d'une connexion sans fil à l'extérieur de deux magasins en Floride.

Avant de se pencher sur l'enjeu des mesures de sécurité, le Commissariat a déterminé si TJX avait un motif raisonnable pour recueillir les renseignements touchés par l'intrusion. Les données de cartes de paiement, y compris les numéros et dates d'expiration de cartes de crédit, étaient nécessaires pour conclure des ventes; par conséquent, il était raisonnable de les recueillir. Toutefois, selon le Commissariat, la collecte des renseignements figurant sur le permis de conduire et d'autres données d'identification provinciales à des fins de retour de marchandises n'était pas nécessaire ni raisonnable dans les circonstances. En accord avec des conclusions précédentes (présentées dans la section 7.1 de ce document), le Commissariat a conclu que TJX aurait dû uniquement recueillir les noms et adresses des clients pour les retours de marchandises et non pas les renseignements figurant sur le permis de conduire ou d'autres données. La collecte des renseignements figurant sur le permis de conduire exposait davantage les personnes au vol d'identité, en plus d'être inutile pour la transaction.

Le Commissariat a ensuite examiné l'enjeu de la conservation des renseignements personnels. TJX avait fait savoir qu'elle conservait les numéros de permis de conduire et les autres numéros d'identification indéfiniment. Le Commissariat a déterminé que puisque TJX n'aurait pas dû a priori recueillir ces renseignements, elle avait encore moins le droit de les conserver. Le Commissariat a recommandé que TJX cesse la collecte de renseignements figurant sur le permis de conduire et d'autres données d'identification pour les retours de marchandises, qu'elle supprime ces renseignements de toutes ses bases de données et qu'elle avise clairement ses clients des raisons pour lesquelles elle recueille certains renseignements personnels, conformément à sa nouvelle politique sur les retours, de l'utilisation qu'elle en fera et de leur éventuelle communication. Le Commissariat a

50 Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels – TJX Companies Inc./Winners Merchant International L.P. – http://www.privcom.gc.ca/cf-dc/2007/tjx_rep_070925_f.asp.

également recommandé que TJX lui soumette un exemplaire de ses nouvelles politiques de conservation.

En réponse aux recommandations du Commissariat quant à la collecte et à la conservation, TJX avança qu'elle avait besoin de recueillir les renseignements sur le permis de conduire à des fins précises, mais qu'à l'avenir, elle allait convertir les numéros du permis en utilisant une fonction de hachage cryptographique. Cette technique permet de convertir chaque numéro de permis en un code unique, appelé « valeur de hachage », ce qui rend impossible l'accès au numéro de permis à tout employé de TJX. Le Commissariat a accepté cette solution en y ajoutant l'obligation de conserver les renseignements du permis de conduire de façon uniquement temporaire.

Finalement, le Commissariat s'est penché sur l'enjeu des mesures de sécurité. Il a examiné « si TJX [avait] mis en place des mesures de protection "raisonnables" et si les risques en matière de sécurité étaient prévisibles. En outre, [il] a tenu compte de la probabilité des dommages, de la gravité du préjudice, du coût des mesures de prévention et des normes pertinentes relatives aux pratiques ». Pour déterminer la gravité potentielle d'un préjudice relié à un cas particulier, le Commissariat a recommandé que les organisations considèrent la nature des renseignements personnels, le nombre de personnes qui pourraient être visées et le temps écoulé avant que l'atteinte à la protection des données ne soit détectée.

Le Commissariat a constaté que TJX avait en place des mesures de protection physiques, administratives et techniques au moment de l'intrusion. Les mesures physiques comprenaient du personnel de sécurité, des cartes d'identité avec photo, des cartes magnétiques, des caméras de surveillance et des verrous de sécurité. Les mesures administratives comprenaient « une structure de gouvernance de la sécurité de l'information supervisée par un dirigeant principal de l'information, un code de conduite à l'intention des employés, un nombre limité d'autorisations de sécurité, une procédure de vérification des antécédents des employés, des procédures permettant de s'assurer que les employés qui quittent l'entreprise remettent leur carte d'identité, leur clé et leur carte magnétique, des cours de formation continue à l'intention des employés, et des politiques et lignes directrices en matière de sécurité ». Puis, en ce qui concerne les mesures de sécurité techniques en place, TJX restreignait l'accès à ses réseaux informatiques notamment à l'aide du chiffrement et de l'accès à distance.

Cependant, le Commissariat a constaté certaines lacunes dans les mesures de sécurité techniques de TJX, comme l'utilisation d'un protocole de chiffrement peu fiable et son échec à implanter une norme de chiffrement plus stricte dans un délai raisonnable. Au moment de la découverte de l'intrusion à la fin de 2006, TJX travaillait toujours à la conversion de son réseau sans fil du protocole WEP (protocole de confidentialité équivalant aux transmissions par fil) au protocole de sécurité Wi-Fi Protected Access (WPA) pour améliorer le chiffrement de ses données. Le Commissariat a fait remarquer que l'utilisation du protocole WEP comme norme de sécurité était remise en question depuis au moins 2003 et que la version 1.1 des normes de sécurité sur les données de l'industrie des cartes de paiement, qui exigeait l'utilisation du protocole de chiffrement WPA, était en circulation depuis septembre 2006. Par conséquent, TJX aurait dû avoir

adopté la norme de l'industrie, une norme beaucoup plus stricte que celle que TJX utilisait, avant la fin de 2006. De plus, TJX avait le devoir de surveiller ses systèmes, et si une surveillance appropriée avait été en place, l'organisation aurait eu connaissance de l'intrusion bien avant.

À la lumière de ces constatations, le Commissariat a conclu que le risque d'intrusion était prévisible et que, dans les circonstances, TJX n'avait pas respecté le principe 4.7 de la LPRPDÉ.

5.2 Autres enquêtes sur les mesures de sécurité

Même si l'enquête visant TJX a établi des lignes directrices importantes pour les organisations qui s'informent de leur obligation de protéger les renseignements personnels, d'autres conclusions d'enquête fournissent des exemples de mesures de sécurité qui sont considérées acceptables ou inacceptables en vertu de la LPRPDÉ *:*

- Une organisation a adéquatement protégé les renseignements personnels en les encodant immédiatement et en limitant l'accès aux numéros de permis de conduire et aux formulaires d'inscription des conducteurs[51];

- Si une organisation reçoit des renseignements sensibles par télécopieur – une pratique que le Commissariat désapprouve généralement –, elle doit avoir en place des mesures de sécurité strictes, comme de s'assurer que le télécopieur qui reçoit les transmissions se trouve dans une pièce dont la porte est verrouillée et dont l'accès est réservé à un nombre limité d'employés qui ont la responsabilité de recevoir les renseignements[52];

- Dans une affaire réglée en cours d'enquête, une personne était inquiète du fait que son numéro de carte de crédit figurait au complet sur un reçu de restaurant. La pratique de

51 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 185 : Les raisons pour lesquelles une compagnie de chemin de fer recueille des renseignements personnels sont jugées appropriées; ses mesures de sécurité sont adéquates – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030512_2_f.asp.

52 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 226 : L'entreprise recueille sans raison valable des renseignements médicaux; les mesures de sécurité sont insuffisantes – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031031_f.asp. Dans cette affaire, la commissaire adjointe a constaté qu'il n'était pas approprié que des agents des ressources humaines ne possédant pas de compétences médicales « reçoivent, annotent, interprètent et traitent, pour administrer le régime d'assurance-invalidité de l'entreprise, des diagnostics médicaux très sensibles » concernant leurs collègues de travail. La collecte de renseignements médicaux confidentiels de l'organisation ne se limitait pas aux renseignements nécessaires aux fins déterminées. L'organisation avait avisé ses employés qu'ils « devaient » lui transmettre les renseignements, mais elle n'avait pas précisé qu'elle n'était pas dans l'obligation de les recueillir et qu'elle le faisait pour faciliter le processus de réclamation. Voir la partie sur la collecte excessive de renseignements médicaux à la section 7.3 de ce document.

l'industrie a changé et tous les numéros de carte de crédit sont masqués sur les reçus[53];

- Un système téléphonique automatisé donnant accès aux cinq transactions les plus récentes d'un compte, uniquement à l'aide du numéro de compte, ne fournit pas une sécurité appropriée pour les renseignements personnels contenus dans les transactions[54];

- Laisser un ordinateur portatif sans surveillance dans un véhicule verrouillé ne constitue pas une mesure de sécurité suffisante, même si l'accès aux renseignements personnels est protégé par un mot de passe[55].

Selon le Commissariat, la présence croissante de la technologie sans fil rend insuffisante la simple protection par un mot de passe des renseignements personnels stockés dans les appareils mobiles; tous les renseignements personnels détenus devraient être encodés selon des normes efficaces, reconnues et approuvées par l'industrie.

Il est important de souligner que la LPRPDÉ ne contient pas actuellement de disposition qui oblige une organisation à notifier les personnes dont les renseignements personnels ont été compromis au cours d'une atteinte à la protection des données. Le Commissariat a demandé que la LPRPDÉ soit modifiée pour inclure une obligation de notification en cas d'atteinte à la protection des données. Il a également préparé des lignes directrices pour la notification en cas d'atteinte à la vie privée en vue d'aider les organisations à décider s'il faut notifier les personnes concernées, et si oui, à quel moment le faire, qui faut-il notifier, de quelle façon et dans quelles circonstances.

53 Exemple de plainte réglée en cours d'enquête nº 25 : Les renseignements personnels figurant sur les reçus des transactions faites par carte de crédit seront masqués d'ici 2007 – http://www.privcom.gc.ca/ser/2006/s25_060127_f.asp.

54 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 292 : Un ancien employeur a changé les renseignements relatifs à un membre du programme pour voyageurs fréquents d'Air Canada – http://www.privcom.gc.ca/cf-dc/2005/292_050406_f.asp.

55 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 289 : Le vol d'un ordinateur portatif met en cause la responsabilité d'une banque – http://www.privcom.gc.ca/cf-dc/2005/289_050203_f.asp.

Principales étapes à suivre par les organisations en cas d'atteinte à la vie privée

Août 2007 – www.privcom.gc.ca/information/guide/2007/gl_070801_01_f.asp

Les quatre principales étapes à suivre en cas d'accès non autorisé aux renseignements personnels, ou de collecte, d'utilisation ou de communication non autorisées de ces renseignements sont présentées ci-dessous.

1re étape *Limitation dans l'atteinte à la vie privée et évaluation préliminaire*
Cette étape consiste à prendre sans tarder des mesures sensées pour limiter l'atteinte à la vie privée, telles que :

- Limiter immédiatement l'atteinte;
- Désigner une personne qualifiée au sein de l'organisation pour la tenue de l'enquête initiale;
- Déterminer s'il est nécessaire de mettre sur pied une équipe composée de représentants des secteurs concernés de l'entreprise;
- Déterminer qui doit être mis au courant de l'incident à l'interne et à l'externe;
- Prévenir la police si l'atteinte semble provenir d'un vol ou d'une autre activité criminelle;
- Ne pas nuire à la capacité d'enquêter sur l'atteinte (c.-à-d. prendre soin de ne pas détruire les éléments de preuve).

2e étape *Évaluation des risques associés à l'atteinte à la vie privée*
Cette étape consiste à évaluer les risques en fonction des facteurs suivants :

i) Les renseignements personnels en cause :

- Quels éléments de données sont en cause?
- Dans quelle mesure les renseignements sont-ils sensibles?
- Quel est le contexte lié aux renseignements personnels en cause?
- Les renseignements personnels sont-ils convenablement encodés, dépersonnalisés ou difficiles d'accès?
- Comment les renseignements personnels peuvent-ils être utilisés?

ii) Cause et étendue de l'atteinte

- Dans la mesure du possible, déterminer la cause de l'atteinte.
- Y a-t-il un risque que l'atteinte se poursuive ou se reproduise, ou que les renseignements soient davantage compromis?
- Quelle a été l'étendue de l'accès non autorisé aux renseignements personnels ou de la collecte, de l'utilisation ou de la communication non autorisée de tels renseignements?
- Les renseignements ont-ils été perdus ou volés? Ont-ils été retrouvés?
- Quelles mesures ont déjà été prises pour atténuer les préjudices?
- S'agit-il d'un problème systémique ou d'un incident isolé?

iii) Personnes concernées par l'atteinte

- Quelle est la quantité de renseignements personnels compromis?
- Qui sont les personnes concernées?

iv) Préjudices prévisibles découlant de l'atteinte

- Quelles étaient les attentes raisonnables des personnes concernées concernant la protection des renseignements personnels?
- Qui est le destinataire des renseignements? Le destinataire est-il connu, digne de confiance et susceptible de rendre les renseignements sans les utiliser ou les communiquer?
- Quels préjudices l'atteinte pourrait-elle causer aux personnes et à l'organisation concernées? Quel préjudice la notification de l'atteinte pourrait-elle causer au public?

3e étape *Notification*

Pour décider s'il convient de notifier les personnes concernées, et si oui, à quel moment, de quelle façon et qui doit le faire, pour décider du libellé de la notification, ainsi que pour décider quelles personnes, tierces parties ou autorités doivent être notifiées, les organisations doivent tenir compte des éléments suivants :

i) Notifier les personnes concernées

- Quelles sont les obligations légales et contractuelles?
- Quels sont les risques de préjudice pour les personnes concernées?
- Y a-t-il un risque raisonnable de vol d'identité ou de fraude (compte tenu, généralement, du type de renseignements perdus, tels que le nom et l'adresse d'une personne combinés à des numéros de pièces d'identité émises par le gouvernement ou la date de naissance)?
- La personne concernée risque-t-elle de subir un dommage physique (risque-t-elle, entre autres, d'être suivie ou d'être victime de harcèlement à la suite de la perte des renseignements personnels)?
- La personne risque-t-elle de subir des humiliations ou des atteintes à la réputation?
- Dans quelle mesure la personne est-elle capable d'éviter ou d'atténuer les préjudices éventuels?

ii) Quand et comment notifier, et qui devrait le faire

- Les personnes concernées par l'incident doivent être notifiées le plus tôt possible après l'évaluation de l'incident.
- Vérifier auprès des autorités si la notification doit être différée pour éviter de compromettre la tenue de l'enquête.
- Il est préférable de notifier directement les personnes concernées, c.-à-d. par téléphone, par la poste, par courriel ou en personne.
- La notification indirecte (comme par des sites Web, des avis publics ou par les médias) ne devrait être utilisée que si la notification directe est susceptible de causer davantage de préjudices, si les coûts afférents sont prohibitifs ou si les coordonnées des personnes concernées sont inconnues.
- L'organisation qui entretient un rapport direct avec le client ou l'employé doit notifier les personnes concernées.
- Dans certaines circonstances, la notification par une tierce partie pourrait mieux convenir (par exemple, dans le cas d'une atteinte à la protection des données de cartes de crédit chez un détaillant, la société émettrice de cartes de crédit peut notifier elle-même les clients concernés puisque le détaillant pourrait ne pas avoir les coordonnées de ceux-ci).

iii) Le libellé de la notification

La notification doit contenir des renseignements, par exemple :

- Des renseignements sur l'incident et le moment où il s'est produit;
- Une description des renseignements personnels en cause;
- Une description sommaire des mesures prises par l'organisation pour maîtriser ou atténuer les préjudices;
- Ce que l'organisation compte faire pour aider les personnes et les mesures que ces dernières peuvent prendre pour éviter ou réduire les risques de préjudice;
- Des sources d'information conçues pour aider les personnes à se prémunir contre le vol d'identité;
- Les coordonnées d'un service ou d'une personne de l'organisation qui peut répondre aux questions ou donner davantage d'information;
- Le cas échéant, préciser si l'organisation a avisé un commissariat à la protection de la vie privée;
- Des coordonnées supplémentaires pour permettre à la personne de faire part de ses inquiétudes à l'organisation;
- Les coordonnées des Commissariats à la protection de la vie privée concernés.

iv) Autres personnes ou organismes à notifier

- Les commissaires à la protection de la vie privée;
- Les policiers, en cas de vol ou d'activité criminelle présumés;
- Les sociétés d'assurances ou autres, s'il est nécessaire de le faire en vertu d'obligations contractuelles;
- Les ordres professionnels ou d'autres organismes de réglementation, si les normes professionnelles ou d'application de la réglementation l'exigent;
- Les sociétés émettrices de cartes de crédit, les institutions financières ou les agences d'évaluation du crédit, si leur aide est requise pour communiquer avec les personnes concernées ou pour atténuer les préjudices;
- Des tiers internes ou externes qui n'ont pas déjà été notifiés;
- Des unités opérationnelles internes qui n'ont pas déjà été notifiées;
- Les syndicats ou autres unités de négociation.

4e étape *Prévention de futures atteintes à la vie privée*

Une fois que les mesures immédiates sont prises pour réduire les risques associés à l'atteinte à la protection des renseignements personnels, les organisations doivent prendre le temps d'enquêter sur les causes de l'incident et de réfléchir à la nécessité d'élaborer un plan de prévention. Plus ou moins d'efforts doivent être déployés en fonction de la gravité de l'incident et de son caractère systémique ou isolé. Le plan peut prévoir ce qui suit :

- Une vérification de la sécurité physique et technique;
- Un examen des politiques et des procédures, ainsi que tout changement témoignant des leçons tirées de l'expérience;
- Un examen des pratiques de formation des employés;
- Un examen des partenaires de la prestation de services.

Pour obtenir plus de renseignements sur les atteintes à la vie privée, y compris la *Liste de contrôle concernant les atteintes à la vie privée* qui a été publiée en août 2007, consultez le site Web du Commissariat à la protection de la vie privée, à l'adresse suivante :

www.privcom.gc.ca/information/guide/2007/gl_070801_01_f.asp.

6. COMMUNICATIONS NÉGLIGENTES ET BESOIN DE FORMATION CONTINUE POUR LES EMPLOYÉS

Bien que les mesures de sécurité soient en grande partie des mesures techniques, les mesures organisationnelles et administratives sont tout aussi importantes. Afin d'éviter des situations de communications négligentes ou par inadvertance de renseignements personnels, les organisations doivent établir des politiques et des procédures de sécurité exhaustives qui mettent l'accent sur la formation continue des employés, particulièrement pour éviter les tentatives de faux-semblant.

6.1 Ingénierie sociale et faux-semblant

Au Canada, l'enquête type en matière de faux-semblant concerne trois grandes entreprises de télécommunications[56]. En 2005, le magazine *Maclean's* a rapporté qu'il avait obtenu des relevés d'appels effectués par la commissaire à partir de son téléphone résidentiel et de son BlackBerry du travail, ainsi que les relevés téléphoniques d'un chef de la rédaction du magazine. *Maclean's* avait acheté ces relevés à l'entreprise américaine Locatecell.com.

Les enquêtes ont révélé que Locatecell.com avait obtenu les relevés de façon illégitime des entreprises canadiennes de télécommunications Bell, TELUS Mobilité et Fido par l'utilisation de l'ingénierie sociale, y compris le faux-semblant. En d'autres mots, Locatecell.com a manipulé les employés des entreprises canadiennes de télécommunications afin qu'ils divulguent des renseignements personnels de clients. Rien ne prouve que les divulgations aient été effectuées par des employés malhonnêtes ou que quiconque ait piraté les systèmes informatiques, comme ce fut le cas dans l'affaire TJX.

Le commissaire adjoint a conclu que les employés des trois entreprises canadiennes de télécommunications n'ont pas respecté les procédures d'authentification de la clientèle mises en place. Il a aussi affirmé que les procédures d'authentification des entreprises et la formation de leurs employés étaient inadéquates et qu'elles ne protégeaient pas suffisamment les renseignements personnels des clients. Les entreprises ont répondu qu'elles mettraient en œuvre les recommandations du commissaire adjoint, à savoir fournir

56 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 372 – Les communications aux courtiers en données exposent les faiblesses des mesures de sécurité en télécommunications – http://www.privcom.gc.ca/cf-dc/2007/372_20070709_f.asp.

une formation supplémentaire aux employés (y compris des renseignements sur les méthodes d'ingénierie sociale), limiter les communications de renseignements personnels par téléphone et améliorer les procédures d'authentification conformément aux lignes directrices en matière d'identification et d'authentification émises par le Commissariat à la protection de la vie privée.

Lignes directrices du CPVP en matière d'identification et d'authentification

Octobre 2006 – http://www.privcom.gc.ca/information/guide/auth_061013_f.asp

Le CPVP a élaboré les lignes directrices ci-dessous pour aider les organisations à développer des processus d'identification et d'authentification appropriés.

- *Authentifier lorsque nécessaire*

Une organisation doit authentifier l'identité d'une personne lorsque la nature de la transaction l'exige.

- *Le niveau d'authentification doit être proportionnel au risque*

La rigueur des processus d'authentification doit être proportionnelle au risque couru par les renseignements devant être protégés, le risque étant fonction de la sensibilité des renseignements ou du service en question, de leur vulnérabilité et de la menace. En outre, le niveau et les méthodes d'authentification peuvent varier selon la nature de l'interaction avec le client.

- *Répondre à la variabilité des menaces*

Les organisations doivent régulièrement réévaluer les risques et les menaces que présente chacun de leurs points de services et prendre les mesures d'atténuation du risque qui s'imposent, y compris le rajustement des processus d'authentification, afin de réagir à la variabilité des menaces. Les organisations doivent également s'assurer que les processus d'authentification en place permettent d'atténuer les risques que peuvent entraîner les nouveaux services.

- *Contrôler régulièrement les menaces*

Les organisations doivent évaluer régulièrement les tentatives d'attaques, les pannes et les pertes de données dans le cadre d'un programme structuré d'évaluation du risque et des menaces, et mesurer la sensibilisation et la confiance des clients à l'égard des processus d'authentification en place.

- *Former les employés*

Les organisations doivent faire en sorte que tous les employés qui ont accès à des renseignements personnels reçoivent une formation appropriée sur l'importance de protéger les renseignements personnels des clients, y compris sur la nécessité de protéger ces données contre l'accès et la communication non autorisés.

- *Rôle des personnes*

Les personnes ont un rôle à jouer dans la protection de leurs renseignements personnels. Il leur incombe de poser des questions et d'éviter le recours à des processus d'authentification non concluants, en choisissant des éléments d'authentification plus rigoureux, ainsi que de toujours protéger leurs identificateurs et authentificateurs.

- *Modifier les données d'authentification*

Les organisations doivent donner aux personnes la possibilité de modifier périodiquement leurs données d'identification ainsi que les authentificateurs qu'elles ont choisis.- *Choix personnels*

Les personnes doivent pouvoir choisir leurs éléments d'identification et d'authentification aux fins de gestion des risques liés à leur identité et à leur droit à la vie privée. Les organisations doivent également offrir aux clients qui en font la demande des processus d'authentification renforcés.

- *Faciles à se rappeler, difficiles à deviner*

Lorsqu'un client choisit un facteur d'authentification basé sur quelque chose qu'il connaît, l'élément d'information doit être facile à retenir ou à masquer, mais difficile pour une autre personne à deviner ou à communiquer. Si certaines personnes estiment qu'elles doivent tenir un registre de leurs mots de passe, il faut les inciter à conserver ce registre dans un endroit sécuritaire, par exemple, dans un fichier informatique chiffré.

- *Éléments d'identification personnels*

Idéalement, l'authentification ne doit pas être basée sur des éléments d'identification personnels ou d'autres renseignements et identificateurs que les clients vont acquérir pendant leur vie et qui ne sont pas facilement ou souvent modifiés.

- *Jetons d'authentification*

Les jetons d'authentification (cartes d'identité, permis de conduire, passeports, etc.) doivent être utilisés uniquement aux fins prévues initialement. Dans les autres cas, une organisation doit se fier à un jeton seulement si elle est convaincue de l'intégrité du processus d'attribution.

- *Intégrité des processus d'authentification*

Les processus d'authentification doivent comporter des mesures de protection qui assurent la confidentialité et l'intégrité des données d'authentification pendant que celles-ci sont validées, puis conservées.

- *Liste maîtresse*

Le processus d'authentification doit comprendre la tenue de registres fiables des transactions d'authentification, y compris la date, l'heure et le résultat obtenu. La quantité d'information recueillie sur la liste maîtresse doit tenir compte des niveaux de risques associés aux renseignements ou aux services.

- *Impartition*

Dans les cas où une organisation impartit le service à la clientèle à un tiers, la responsabilité principale de garantir que les processus d'identification et d'authentification sont adéquats revient quand même au fournisseur de service que le client a choisi. Même si l'authentification comme telle est effectuée par le tiers, l'organisation conserve la responsabilité de garantir que les processus d'authentification satisfont à ses exigences et d'assurer la protection des renseignements et des biens des clients.

6.2 Erreurs négligentes

Mis à part les tentatives de tiers fraudeurs ou de pirates informatiques rusés, beaucoup de renseignements sont malencontreusement communiqués sans autorisation par des employés à la suite d'une négligence ou en raison d'un manque de formation[57]. Plusieurs examens de plaintes et d'incidents importants ont permis d'établir des lignes directrices éclairantes sur l'utilisation adéquate des mesures de sécurité et sur le besoin de former les employés.

Dans les trois premiers résumés d'incidents en vertu de la LPRPDÉ, le Commissariat a conclu que la LPRPDÉ avait été transgressée lorsque des renseignements personnels avaient été envoyés par télécopieur aux mauvais numéros. Dans un cas, des télécopies contenant des renseignements personnels sur la santé ont été envoyées par erreur au concierge d'un immeuble[58]. Dans d'autres cas, des télécopies contenant des renseignements bancaires ont été envoyées par inadvertance à des entreprises et à des personnes à Montréal, à Dorval et aux États-Unis pendant plusieurs années[59]. Des cas de télécopies envoyées par erreur continuent de se produire et de contrevenir à la LPRPDÉ[60] et des cas de courriels envoyés par erreur ont aussi été constatés[61]. Les négligences de ce type sont un problème d'envergure.

L'élimination inadéquate de renseignements personnels est également inquiétante. La commissaire adjointe a conclu que le fait de jeter des renseignements personnels bancaires de nature délicate dans un bac de recyclage contrevient à la LPRPDÉ[62]. Dans l'affaire en question, le plaignant a appris que ses renseignements personnels bancaires avaient été trouvés par une tierce partie dans le bac de recyclage non surveillé d'un stationnement. Les renseignements comprenaient les noms, l'adresse, les numéros d'assurance sociale et le numéro de compte du plaignant et de sa femme, ainsi que leur historique de transactions. La banque a déterminé que deux membres du personnel, à qui on avait confié la tâche de vider le bureau d'un ancien employé, avaient jeté par inadvertance des

57 *Richard Breithaupt et Peggy Fournier c. Hali MacFarland et Calm Air International ltd.* (numéro de dossier de la Cour fédérale T-2061-04). Cette affaire porte sur la communication alléguée de renseignements sur l'itinéraire des plaignants par une employée d'une compagnie aérienne à un agent de la GRC. L'affaire a été réglée au cours du processus de médiation avec la commissaire en 2005.

58 Résumé d'incident nº 1 – Des télécopies contenant des renseignements médicaux sont envoyées par erreur aux concierges d'un immeuble à appartements – http://www.privcom.gc.ca/incidents/2004/041221_f.asp.

59 Résumé d'incident nº 2 – Défaillance des pratiques de la CIBC en matière de protection des renseignements personnels lors d'envois de documents par télécopieur – http://www.privcom.gc.ca/incidents/2005/050418_01_f.asp; résumé d'incident nº 3 – Documents acheminés par télécopieur aux mauvaises personnes – http://www.privcom.gc.ca/incidents/2006/003_061204_f.asp.

60 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 332 – Une banque communique de nouvelles directives et sensibilise ses employés après que des renseignements sur des clients eurent été envoyés par télécopieur au mauvais destinataire – http://www.privcom.gc.ca/cf-dc/2006/332_20060412_f.asp.

61 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 360 – Une banque envoie par erreur à une cliente, dans un courrier électronique, des renseignements personnels concernant des employés – http://www.privcom.gc.ca/cf-dc/2006/360_20061114_f.asp.

62 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 356 – Les renseignements personnels bancaires d'un client sont trouvés dans un bac de recyclage – http://www.privcom.gc.ca/cf-dc/2006/356_20061023_f.asp.

documents contenant ces renseignements dans un bac de recyclage plutôt que dans un bac de déchiquetage. Selon la commissaire adjointe, l'organisation a dérogé à la disposition relative aux mesures de sécurité de la LPRPDÉ. La commissaire adjointe s'est également dite inquiète que des documents contenant des renseignements personnels aient été abandonnés dans le bureau d'un ancien employé pendant un an. Elle a recommandé que de tels documents soient déchiquetés dans le cadre d'une approche systématique visant à traiter les renseignements confidentiels confiés à un employé lorsque celui-ci quitte l'organisation.

De nombreuses autres enquêtes ont permis d'établir des lignes directrices utiles concernant les exigences de la LPRPDÉ en matière de communications par inadvertance et de formation des employés. Ces enquêtes peuvent être résumées en quelques mots par les principes ci-dessous. Bien que certains de ces principes découlent de circonstances particulières, les règles élaborées au cours des enquêtes ont une portée générale :

- Les employés ne peuvent pas manipuler les renseignements liés à la paye de leurs collègues sans signer d'accord de confidentialité ni recevoir de formation, et sans autres mesures de sécurité appropriées en place[63];

- Les organisations contreviennent à la LPRPDÉ lorsqu'elles ne sensibilisent pas leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels[64];

- L'utilisation d'une seule mesure de sécurité pour confirmer l'identité du propriétaire d'un coffret de sûreté – un numéro consigné sur une carte de signature – n'est pas suffisante lorsqu'un client peut ouvrir par erreur un coffret de sûreté qui ne lui appartient pas[65];

- Communiquer des renseignements financiers au fiancé ou à la fiancée d'un client ou d'une cliente, ou laisser un dossier ouvert sur un bureau de la banque, sans avoir vérifié si le ou la fiancé(e) possède l'autorisation écrite d'agir au nom du client de la banque, est contraire à la LPRPDÉ[66];

63 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 242 – Un homme s'oppose à ce que des travailleurs assignés temporairement traitent les renseignements liés à la paye – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031204_06_f.asp.

64 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 54 – Un couple prétend qu'il y a eu communication inappropriée de leur dossier téléphonique à un tiers – http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020628_2_f.asp.

65 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 344 – Le coffret de sûreté d'un couple ouvert par erreur – http://www.privcom.gc.ca/cf-dc/2006/344_20060717_f.asp.

66 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 200 – Mariage annulé à la suite d'une communication de renseignements par la banque – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_01_f.asp.

- Communiquer des renseignements sur le compte en souffrance d'un client à la personne qui lui a recommandé l'organisation, mais qui ne possède pas l'autorisation d'agir en son nom, est contraire à la LPRPDÉ[67];

- Utiliser un système automatisé pour laisser un message sur le répondeur d'une personne (sans son autorisation) pour lui communiquer des renseignements sur sa facture de carte de crédit en souffrance, même si ces renseignements sont utiles, est contraire à la LPRPDÉ, car le message peut être entendu par toute personne ayant accès au répondeur[68];

- Envoyer par erreur des renseignements financiers sensibles dans une enveloppe non scellée est contraire aux dispositions relatives aux mesures de sécurité de la LPRPDÉ[69].

Comme le démontrent les enquêtes types citées dans cette section, les employés d'une organisation peuvent faire des erreurs négligentes qui entraînent des communications non autorisées de renseignements personnels. Ces erreurs peuvent être aussi nuisibles à une organisation et aux personnes concernées que des attaques intentionnelles ou des atteintes à la protection des données.

Les organisations doivent se pencher sur le facteur humain de leurs opérations et s'assurer que leurs employés ne sont pas le maillon le plus faible de leur système de sécurité. Des politiques, des procédures et des séances de formation appropriées sont essentielles à un programme de sécurité. Les employés doivent recevoir une formation sur la façon adéquate de recueillir, d'utiliser et de communiquer les renseignements personnels au moment de leur embauche ainsi que de façon régulière. La formation continue des employés est essentielle à la protection efficace des renseignements personnels.

67 Exemple de plainte réglée en cours d'enquête nº 27 – Une clinique (dentaire) communique les renseignements d'une cliente en tentant de recouvrer une créance – http://www.privcom.gc.ca/ser/2006/s27_060516_f.asp.

68 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 270 – La banque accepte de changer son message automatisé – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040504_f.asp.

69 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 154 – Consternation chez un couple qui reçoit une enveloppe non scellée de sa banque – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030415_1_f.asp.

7. COLLECTE EXCESSIVE DE RENSEIGNEMENTS

Sous réserve de certaines exceptions prévues à l'article 7 de la LPRPDÉ, le principe 4.3 stipule que les organisations doivent obtenir le consentement de la personne pour recueillir, utiliser et communiquer des renseignements personnels qui la concernent. En vertu du principe 4.4, les organisations ne peuvent recueillir que les renseignements personnels nécessaires aux fins déterminées, et le principe 4.4.1 interdit la collecte de renseignements personnels de façon arbitraire.

De nombreuses enquêtes types ont contribué à définir la quantité et la nature des renseignements personnels qui peuvent être recueillis dans différentes situations.

7.1 Retours de produits et utilisation d'une carte de crédit

Dans le secteur du commerce de détail, un grand nombre d'organisations exigent que leurs clients montrent une pièce d'identité pour retourner ou échanger un produit. En général, la collecte de ces renseignements vise à prévenir les fraudes et les erreurs. Dans une enquête type relative à l'exigence de fournir une carte d'identité avec photo pour un remboursement ou un échange, le Conseil canadien du commerce de détail a donné quelques exemples qui illustrent pourquoi la collecte de renseignements personnels sur les clients est nécessaire pour lutter contre le vol et la fraude :

- Réduction du vol par les employés – Les employés ne peuvent plus prétendre qu'un article a été retourné à des fins de remboursement par une personne inconnue. L'information au sujet du client est maintenant disponible et les magasins peuvent vérifier le retour de la marchandise;

- Consignation de multiples retours effectués par la même personne ou par des personnes qui ont des noms différents, mais qui vivent à la même adresse ou qui ont le même numéro de téléphone;

- Établissement de modèles de consommation – Par exemple, les gens peuvent acheter un article et en utiliser la moitié. Ils retournent ensuite la portion non utilisée et prétendent que

l'article est défectueux ou n'était pas complet au moment de l'achat;

- Réduction des « vols basés sur des reçus » – Il s'agit du vol d'articles inscrits sur des reçus qu'on peut trouver à l'extérieur du magasin ou dans un centre commercial[70].

L'enjeu dans cette affaire consistait à déterminer si l'exigence de fournir une carte d'identité avec photo était raisonnable aux fins de lutte contre la fraude et si les personnes étaient informées de la collecte et y avaient accordé leur consentement explicite[71].

Selon la commissaire adjointe, la perte de vie privée était minimale, puisque les renseignements figurant sur la carte d'identité avec photo, qui étaient demandés au client, n'étaient pas consignés par le magasin. La commissaire adjointe en est venue à la conclusion qu'il n'existait pas d'autre façon de prévenir la fraude et que les objectifs du magasin étaient appropriés dans les circonstances. Dans le cas où un magasin voudrait faire de la présentation d'une carte d'identité avec photo une condition pour les remboursements ou les échanges, il devrait explicitement énoncer ses objectifs en vertu du principe 4.3.3.

Bien qu'à plusieurs endroits dans le magasin il était clairement indiqué qu'il fallait présenter une carte d'identité avec photo pour les remboursements et les échanges, la commissaire adjointe a constaté qu'on n'expliquait nulle part pourquoi une carte d'identité avec photo était requise. Par conséquent, elle a conclu que l'organisation ne respectait pas les exigences concernant le consentement explicite de la LPRPDÉ, lesquelles exigent que la personne soit informée des fins auxquelles les renseignements seront utilisés. Le Commissariat a recommandé au magasin d'expliquer dans sa politique sur les retours les raisons pour lesquelles la présentation d'une carte d'identité avec photo et la collecte d'autres renseignements personnels sont requises au moment du remboursement ou de l'échange de produits, à savoir pour éviter les fraudes.

70 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 361 : Un détaillant exige une carte d'identité avec photo pour échanger un article – http://www.privcom.gc.ca/cf-dc/2006/361_20061114_f.asp.

71 Le magasin a aussi demandé au client de donner son nom, son adresse et son numéro de téléphone. Même si le plaignant ne s'était pas opposé à donner ces renseignements, la commissaire adjointe a quand même examiné la question. Elle a déterminé que la collecte de ces renseignements entraînait une perte minimale de vie privée et était donc appropriée dans les circonstances.

Fiche d'information : Directive sur l'identification avec photo
Septembre 2007 – http://www.privcom.gc.ca/fs-fi/02_05_d_34_tips_f.asp

Avec la collaboration des commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, le Commissariat à la protection de la vie privée du Canada a publié une fiche d'information en septembre 2007 à l'égard de l'utilisation de l'identification avec photo pour l'achat de biens avec une carte de crédit.

Les commissariats acceptent que les organisations exigent de leurs clients qui souhaitent payer des biens et des services par carte de crédit qu'ils montrent une pièce d'identité avec photo. Toutefois, les commissariats ont précisé que « [la] vérification des renseignements personnels doit se limiter à l'examen de l'identité; il est interdit de consigner les renseignements personnels figurant sur la pièce d'identité examinée (par exemple, le numéro du permis de conduire, l'adresse) ». La pratique mentionnée ici vise à établir un équilibre entre le droit à la protection de la vie privée des personnes et le besoin des organisations de prévenir les fraudes par carte de crédit.

7.2 Ouverture de comptes et activités connexes

De nombreuses enquêtes concernant l'ouverture de comptes et les activités connexes ont permis de définir les paramètres servant à déterminer quels renseignements peuvent être recueillis et à quelles fins. Voici un résumé des principes qui se dégagent de ces enquêtes types :

- Un avis de cotisation n'est pas requis à des fins de vérification du revenu concernant la garantie d'une marge de crédit ou l'obtention d'un prêt supplémentaire, car l'avis contient des renseignements qui ne sont pas nécessaires pour le but visé[72];

- Un magasin de location de DVD ne doit pas inscrire dans sa base de données les renseignements figurant sur le permis de conduire ou d'autres renseignements identificateurs pour ouvrir un compte pour un membre[73];

- Les personnes ne sont pas tenues de fournir leur numéro d'assurance social pour louer un appartement[74] ou pour disposer d'une connexion Internet[75];

72 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 169 : Un particulier conteste la demande de la banque de lui fournir un avis de cotisation à des fins de vérification du revenu – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030424_2_f.asp.

73 Exemple de plainte réglée en cours d'enquête nº 28 : Un magasin de location de DVD revoit son processus de demande d'adhésion – http://www.privcom.gc.ca/ser/2006/s28_061214_f.asp.

74 Exemple de plainte réglée en cours d'enquête nº 19 : Les éventuels locataires ne sont pas tenus de fournir leur numéro d'assurance sociale pour louer un appartement – http://www.privcom.gc.ca/ser/2006/s19_060203_f.asp.

75 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 22 : Une entreprise demande le NAS d'une cliente en vertu d'une politique – http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011105_02_f.asp.

- En ce qui a trait au traitement d'une demande d'indemnisation pour vol de biens personnels, une organisation ne peut pas exiger d'une personne qu'elle consente à la collecte de renseignements sur ses antécédents en matière de crédit, sur ses finances, sur sa santé, sur son dossier de conducteur et sur son emploi. Ces renseignements ne sont pas nécessaires pour traiter ce type de demande[76].

7.3 Collecte de renseignements sur la santé

Au cours de diverses enquêtes liées à l'emploi et à la collecte de renseignements sur la santé, le Commissariat à la protection de la vie privée a contribué à déterminer la quantité de renseignements personnels que les organisations doivent recueillir pour administrer des régimes d'avantages sociaux, accorder des congés de maladie et gérer d'autres types d'activités.

Durant l'une de ces enquêtes, le Commissariat a reconnu qu'il était approprié pour les organisations d'exiger un certificat médical pour un congé de maladie prolongé. Cependant, on ne peut exiger des employés qu'ils fournissent à leur employeur des renseignements diagnostiques sur leur état ou sur leur maladie. La note du médecin est suffisante[77].

Lors d'une enquête similaire, le Commissariat a déterminé que la collecte de renseignements sur la maladie d'un employé était abusive puisqu'elle n'était pas nécessaire. Il a conclu que le certificat médical fourni par le médecin de l'employé aurait dû suffire à confirmer que l'absence était justifiée[78].

Par contre, le Commissariat a fait remarquer qu'il était approprié pour l'organisation de demander la date prévue du retour au travail d'un employé afin qu'elle puisse planifier en conséquence (à condition que la demande soit formulée clairement et qu'elle énonce bien que l'organisation cherche à obtenir un pronostic et non un diagnostic)[79].

76 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 368 : Formulaire de consentement d'un expert en assurances jugé trop général – http://www.privcom.gc.ca/cf-dc/2007/368_20070111_f.asp.

77 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 257 : Les employés s'opposent à l'obligation imposée par l'entreprise d'avoir un diagnostic médical sur les certificats de congé de maladie – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031009_01_f.asp.

78 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 233 : Une personne s'objecte à l'exigence de faire part du diagnostic médical sur son certificat d'absence pour congé de maladie – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031003_f.asp.

79 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 135 : Une personne a allégué qu'un employeur avait demandé trop de renseignements médicaux – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030306_4_f.asp.

Lors d'une autre enquête, la commissaire adjointe a déterminé que le conseiller en santé et sécurité du travail d'une organisation ne peut pas communiquer avec un centre hospitalier pour demander des renseignements au sujet de l'examen qu'a subi un employé sans le consentement de ce dernier[80].

80 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 235 : Une personne conteste le refus de son employeur de lui accorder un congé de maladie – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031107_03_f.asp.

8. MEILLEUR ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Sous réserve de certaines exceptions énoncées à l'article 9 de la LPRPDÉ, le principe 4.9 stipule que les organisations doivent informer les personnes qui en font la demande de l'existence de renseignements personnels qui les concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et leur permettre de les consulter.

L'article 8 de la Loi prévoit que les organisations saisies de la demande d'accès doivent y donner suite dans les trente jours suivant sa réception. Cet article stipule également que les organisations peuvent exiger des droits pour répondre à la demande à condition qu'elles informent les demandeurs du montant approximatif des droits et que les demandeurs ne retirent pas leur demande. Cependant, le principe 4.9.4 précise aussi que les organisations doivent fournir les renseignements demandés sans frais, sinon à un coût minime. Plusieurs enquêtes ont permis de résoudre d'importantes préoccupations en matière de droit d'accès aux renseignements personnels, y compris des enquêtes pour lesquelles une action en justice a été intentée en parallèle et des enquêtes relatives à des frais d'accès.

8.1 Principes généraux relativement à l'accès

Dans une enquête concernant une demande d'accès à des renseignements personnels effectuée auprès d'un avocat d'un cabinet, la commissaire adjointe a déclaré que les organisations doivent établir des pratiques et des procédures pour le traitement des demandes d'accès dans le cadre d'un programme global de protection des renseignements personnels[81]. L'avocat en question a carrément refusé de communiquer au plaignant toute forme de renseignements, mais n'a cité aucune des dispositions de la LPRPDÉ pour expliquer ce refus. Il n'a pas non plus transmis la demande du plaignant au responsable de la protection de la vie privée du cabinet. À la suite de l'intervention de la commissaire adjointe, le cabinet a informé son personnel que toute demande d'accès à des renseignements personnels doit être acheminée au responsable de la protection de la vie privée du cabinet. La commissaire adjointe a approuvé cette mesure et conclu que cette

81 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 367 : Importance mise sur le besoin d'établir des procédures pour le traitement de l'accès aux renseignements personnels – http://www.privcom.gc.ca/cf-dc/2007/367_20070119_f.asp.

dernière permettrait à ce cabinet d'avocats de répondre à de futures demandes d'accès aux renseignements personnels conformément à ses obligations en vertu du principe 4.9.

Dans une autre affaire, la Cour fédérale a déterminé que la LPRPDÉ ne garantit pas que les personnes puissent avoir accès à leurs renseignements personnels sous une forme particulière[82]. Si les renseignements contenus dans un document sont conservés dans un autre format que celui dans lequel ils avaient été recueillis initialement, la possibilité d'accéder aux renseignements sous cette autre forme est suffisante pour respecter l'obligation relative à l'accès en vertu de la Loi.

8.2 Incidence des actions en justice intentées en parallèle

Les conclusions d'enquête en vertu de la LPRPDÉ découlent manifestement de la conviction que le droit d'accès aux renseignements est un droit fondamental, quel que soit le motif de la personne qui demande l'accès. Ce droit est fondamental même dans les situations où une personne demande en vertu de la LPRPDÉ à avoir accès à des documents susceptibles d'être pertinents dans le cadre d'actions en justice intentées en parallèle. Certaines organisations ont refusé de donner accès à des renseignements au motif qu'une personne ne devrait pas pouvoir obtenir, par la seule invocation de la LPRPDÉ, des documents qu'elle devrait chercher à obtenir conformément aux règles générales de communication établies par la procédure civile. Dans le cadre de plusieurs enquêtes, le Commissariat a conclu que les actions civiles intentées en parallèle entre les parties ne doivent pas invalider la LPRPDÉ. Nonobstant les litiges en cours, les organisations doivent continuer de recevoir et de traiter les demandes d'accès aux renseignements personnels conformément à leurs obligations au titre de la Loi. Les actions en justice ne doivent pas empêcher systématiquement de tenir compte du droit indépendant d'une personne d'accéder à ses renseignements personnels en vertu de la LPRPDÉ. Les règles traditionnelles de la preuve, telles que les règles de pertinence et les règles contre la pêche aux renseignements dans le cadre d'un litige, ne doivent pas non plus limiter la quantité de renseignements personnels auxquels les personnes ont accès individuellement en vertu de la LPRPDÉ. Sauf si les documents demandés font l'objet d'une exception applicable, les organisations sont tenues de fournir à l'intéressé l'accès à ces documents aux termes de la LPRPDÉ. La communication des renseignements personnels peut être refusée dans les cas suivants : les renseignements sont protégés par le secret professionnel (alinéa 9(3)*a*))[83], la communication révélerait des renseignements commerciaux confidentiels (alinéa 9(3)*b*)) ou les renseignements ont été fournis uniquement à l'occasion d'un règlement officiel des différends (alinéa 9(3)*d*)).

Dans une enquête type portant sur l'accès et sur un litige, le Commissariat s'est penché sur l'histoire d'une entreprise de transport aérien qui a dans un premier temps refusé de

82 *Vanderbeke c. Banque Royale du Canada*, 2006 CF 651 (CanLII) – http://www.canlii.org/fr/ca/cfpi/doc/2006/2006cf651/2006cf651.html.

83 Aux fins d'interprétation ou d'application de la LPRPDÉ, le terme « secret professionnel » a été utilisé pour inclure à la fois le secret relatif au conseil juridique et le privilège relatif au litige. Voir *Blank c. Canada (ministre de la Justice),* 2006 CSC 39, qui a été appliqué dans l'arrêt *Rousseau c. Wyndowe*, 2006 CF 1312 (CanLII) au paragraphe 34, ayant fait l'objet d'un appel pour différents motifs.

communiquer à une personne ses renseignements personnels en réponse à une demande en vertu de la LPRPDÉ[84]. L'entreprise n'a pas traité la demande d'accès conformément à la Loi, mais a décidé de la traiter dans le cadre de la poursuite intentée par le plaignant. L'entreprise de transport aérien a fait valoir son point de vue, selon lequel lors d'un litige, certaines règles et procédures bien définies régissent la communication de documents dans le cadre de poursuites civiles. Selon elle, la Loi ne doit pas avoir préséance sur ces règlements. Selon une conclusion importante qui règle une partie des incohérences pouvant se manifester entre la communication de documents dans le cadre d'un litige et la LPRPDÉ, la commissaire adjointe a fait remarquer que la LPRPDÉ continue de s'appliquer nonobstant toute action civile qui pourrait être en cours au même moment, et que *toutes* les demandes d'accès doivent être examinées à part entière, sous réserve des exceptions applicables au titre de la Loi. La commissaire adjointe a conclu que l'entreprise de transport aérien avait enfreint la Loi pour ne pas avoir examiné et traité la demande d'accès en vertu des règles de la LPRPDÉ et pour ne pas avoir communiqué les renseignements personnels en temps opportun tel qu'il est indiqué dans la Loi, sous réserve des exceptions prévues par la Loi qui peuvent s'appliquer dans les circonstances particulières.

Dans une autre affaire, un médecin a fait subir un examen médical indépendant à une personne pour le compte d'une compagnie d'assurance[85] et a refusé de fournir à cette personne les notes qui avaient été prises pendant l'examen et qui contenaient des renseignements personnels la concernant. Le médecin a affirmé que ses notes étaient soustraites à l'obligation de communication en vertu de l'alinéa 9(3)*a*), qui prévoit qu'une organisation n'est pas tenue de donner accès aux renseignements personnels s'ils sont protégés par le secret professionnel, ou en vertu de l'alinéa 9(3)*d*), puisque les renseignements avaient été obtenus à l'occasion d'un règlement officiel des différends. La commissaire adjointe a rejeté l'argument du médecin qui invoquait les deux exceptions. Elle a souligné que, dans le contexte de la présente plainte, la compagnie d'assurance avait retenu les services du médecin à titre d'expert simplement pour évaluer une demande de prestations aux termes d'une police d'assurance collective. Puisque aucune contestation par les parties n'avait lieu, l'examen n'a pas été effectué dans le contexte d'un litige, voire d'un litige éventuel. De la même manière, un examen médical indépendant, effectué dans le cadre de l'examen et du traitement habituels des demandes, ne peut pas être considéré comme ayant eu lieu à l'occasion d'un règlement officiel des différends.

84 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 352 : Une entreprise de transport aérien tarde à accorder à une personne l'accès à ses renseignements personnels en raison d'un litige en cours – http://www.privcom.gc.ca/cf-dc/2006/352_20060908_f.asp. Voir aussi une affaire précédente qui évoque la même idée dans le cadre d'actions en justice intentées par une personne contre son ancien employeur : Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 285 : Une compagnie refuse à un employé une demande d'accès – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_041221_01_f.asp.

85 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 306 : Un médecin refuse à un patient l'accès à ses renseignements personnels – http://www.privcom.gc.ca/cf-dc/2005/306_20050317_f.asp.

Les conclusions de la commissaire adjointe ont été confirmées par la Cour fédérale[86]. La Cour a indiqué que pour que l'exemption relative au privilège des communications dans un litige puisse s'appliquer dans le but de refuser une demande d'accès aux renseignements personnels en vertu de la LPRPDÉ, il doit être démontré 1) qu'un litige était raisonnablement prévisible au moment de la communication en cause et 2) que le litige était le principal objet de cette communication, conformément à l'alinéa 9(3)*a*). Dans cette affaire, la Cour a tranché que le principal objet de l'examen médical indépendant n'était pas un litige; celui-ci visait plutôt à vérifier si le plaignant était en droit de percevoir des prestations d'invalidité.

Dans le même ordre d'idées, la Cour a déclaré que rien dans la preuve ne permet de croire que l'examen médical indépendant commandé par un assureur constitue une indication qu'un processus de règlement officiel des différends est en cours. Au contraire, la Cour a fait remarquer que l'obligation de se soumettre à un examen médical faisait partie intégrante du contrat d'assurance. La lettre de l'assureur informant M. Rousseau (le plaignant) de la décision de mettre fin à ses prestations indiquait que ce dernier pouvait faire appel de cette décision. Cela signifiait que M. Rousseau avait la possibilité de déclencher un processus officiel de règlement des différends en interjetant appel. Toutefois, ce processus ne pouvait être lancé qu'après avoir reçu la décision de l'assureur laquelle, à son tour, ne pouvait être formulée qu'après l'examen médical indépendant.

8.3 Droits d'accès

Plusieurs enquêtes établissant un précédent ont fourni des lignes directrices utiles sur l'enjeu de réclamer des droits en contrepartie de l'accès aux renseignements personnels. Bien que l'article 8 de la LPRPDÉ permette à une organisation d'exiger des droits pour traiter une demande d'accès, le principe 4.9.4 stipule que l'accès doit être fourni sans frais, sinon à un coût minime. La LPRPDÉ ne précise ni le montant de ces droits ni la façon de les calculer.

Dans une affaire, une personne s'est plainte qu'une organisation avait inclus une estimation des coûts de l'ordre de 1 500 $ pour répondre à sa demande, car la demande était « à l'emporte-pièce » et demandait pour ainsi dire une « vérification judiciaire »[87]. La commissaire adjointe a rejeté catégoriquement le montant de 1 500 $, puisque, en vertu de la LPRPDÉ, l'organisation ne peut exiger pour répondre à la demande « que des droits minimes » ou n'en exiger aucun. Du point de vue de la commissaire adjointe, la LPRPDÉ laisse entendre que les frais doivent être symboliques, et 1 500 $ ne représentent aucunement un montant symbolique.

86 *Rousseau c. Wyndowe*, 2006 CF 1312 (CanLII), ayant fait l'objet d'un appel pour différents motifs – http://www.canlii.org/fr/ca/cfpi/doc/2006/2006cf1312/2006cf1312.html.

87 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 285 : Une compagnie refuse à un employé une demande d'accès – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_041221_01_f.asp.

Dans le cadre d'une autre affaire, une personne s'est plainte qu'une banque exigeait des frais fixes de 25 $ pour traiter toute demande d'accès aux renseignements personnels[88]. La commissaire adjointe a considéré que la pratique de la banque d'exiger des frais fixes pour une demande d'accès était contraire à l'esprit de la Loi. La commissaire adjointe a précisé qu'une organisation devrait seulement considérer exiger des frais pour traiter une demande lorsqu'elle s'est assurée que la demande constituait un cas exceptionnel, et seulement à un coût minime. Elle a conclu que l'objectif de la banque de faire renoncer les gens à leurs demandes d'accès contrevenait à l'objectif de la politique de droits d'accès.

Étant donné que les organisations doivent assumer les coûts des copies de dossiers contenant des renseignements personnels, la commissaire adjointe a recommandé d'autres façons pour que les organisations puissent réduire les coûts et s'acquitter de leur obligation d'offrir l'accès à des renseignements personnels[89]. Dans cette affaire, une organisation exigeait des droits de 20 $ pour demander le dossier à l'entreprise d'entreposage de tierce partie, ainsi que des frais de photocopie de 0,20 $ la page. Puisque le dossier comptait plus de 1 000 pages, l'organisation demandait une somme de 225 $ pour l'obtenir. Pour ce qui est des frais d'entreposage, la commissaire adjointe estimait qu'ils ne devraient pas être pris en compte dans les droits réclamés par l'organisation. L'entreposage des dossiers relève de la responsabilité de l'organisation et, tout comme les autres coûts associés aux activités commerciales, le client ne devrait pas avoir à en payer les frais. Même si la commissaire adjointe était prête à convenir que les frais de photocopie de 0,20 $ la page étaient raisonnables dans les circonstances, elle a fortement recommandé à l'organisation d'envisager d'autres options moins coûteuses pour offrir l'accès à des renseignements personnels. La Loi n'oblige pas une organisation à fournir des copies de renseignements personnels, mais plutôt l'*accès* à ces renseignements. Par exemple, l'organisation pourrait permettre aux personnes d'examiner les dossiers sur place dans le but d'obtenir les renseignements dont elles ont besoin ou de déterminer plus exactement quels documents devraient être photocopiés. Par conséquent, les frais de photocopie susmentionnés ne s'appliqueraient qu'aux copies qui ont été demandées et produites.

Une autre affaire intéressante impliquait une société d'entreposage de dossiers médicaux offrant ses services aux médecins qui prennent leur retraite ou qui quittent la province, mais qui sont tenus par leur organisme de réglementation professionnelle de conserver l'original des dossiers médicaux d'un patient dans un endroit sûr pendant un certain nombre d'années[90]. La commissaire adjointe a déterminé que la société d'entreposage imposait des droits d'accès raisonnables qui correspondent au barème recommandé par l'Association médicale de l'Ontario. Cependant, comme pour l'affaire précédente, elle a fortement recommandé à l'organisation d'envisager d'autres options moins coûteuses pour offrir l'accès à des renseignements personnels. La société d'entreposage

88 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 283 : Une banque exige des frais pour traiter les demandes de renseignements personnels – http://www.privcom.gc.ca/cf-dc/2004/cf-dc_041021_02_f.asp.

89 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 354 : Droits d'accès remis en cause – http://www.privcom.gc.ca/cf-dc/2006/354_20061025_f.asp.

90 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 328 : Une société d'entreposage de dossiers médicaux revoit sa politique d'accès – http://www.privcom.gc.ca/cf-dc/2006/328_20060609_f.asp.

de dossiers médicaux a accepté de modifier sa politique sur la protection de la vie privée pour permettre aux patients de consulter gratuitement leur dossier médical. La société n'imposera des frais que pour les photocopies et pour le transfert des dossiers médicaux personnels à un nouveau médecin. Par conséquent, la commissaire adjointe a conclu que la plainte concernant les frais déraisonnables imposés pour l'accès aux dossiers médicaux était résolue[91].

91 Même si la plainte portait essentiellement sur l'accès, elle a soulevé beaucoup d'autres enjeux stratégiques importants auxquels la commissaire adjointe a fait référence dans ses conclusions.

9. FINS SECONDAIRES DE MARKETING

Les organisations recueillent parfois des renseignements personnels pour la prestation d'un service prévu dans un contrat et souhaiteraient par la suite utiliser ou communiquer ces renseignements à des fins secondaires de marketing. Cette pratique peut être très rentable du point de vue de l'organisation, mais elle n'est pas toujours souhaitable du point de vue des clients potentiels. Certaines organisations font elles-mêmes du marketing secondaire, d'autres communiquent les renseignements à des tiers.

En vertu de la LPRPDÉ, le marketing secondaire peut soulever de nombreux enjeux en matière de renseignements personnels, y compris des questions sur le consentement positif ou négatif, les attentes raisonnables de la personne (principe 4.3.5), le consentement excédant les motifs de la prestation d'un service (principe 4.3.3), le caractère adéquat de l'information et du consentement en général (principes 4.3 et 4.3.2), le moment de préciser les fins de la collecte, de l'utilisation ou de la communication (principes 4.2.3 et 4.3.1), le droit au retrait du consentement (principe 4.3.8) et le caractère acceptable des fins de marketing (paragraphe 5(3)).

Depuis l'entrée en vigueur de la LPRPDÉ, plusieurs enquêtes importantes sur l'utilisation des renseignements personnels des clients à des fins secondaires de marketing ont été entreprises. Le Commissariat a formulé des conclusions pertinentes pour de nombreuses industries en tenant compte des réalités de chacun des secteurs, comme les télécommunications, le commerce de détail, les services bancaires et les compagnies aériennes. Ces conclusions peuvent fournir des lignes directrices utiles pour les organisations désirant utiliser les renseignements personnels recueillis à des fins secondaires.

9.1 Télécommunications

L'affaire *Englander c. TELUS*[92] a traité, entre autres, du consentement des nouveaux abonnés à ce que TELUS utilise à des fins secondaires des renseignements personnels destinés à un annuaire. La Cour d'appel fédérale a conclu que, compte tenu des circonstances, les nouveaux abonnés n'avaient pas donné, ni ne pouvaient avoir donné, un

92 *Englander c. Telus Communications Inc.*, 2004 CAF 387 (CanLII), (2004), 247 D.L.R. (4th) 275 • (2004), 1 B.L.R. (4th) 119 • (2004), 36 C.P.R. (4th) 385 – http://www.canlii.org/fr/ca/caf/doc/2004/2004caf387/2004caf387.html.

consentement valable à ce que TELUS utilise leurs renseignements personnels à toutes les autres fins[93]. Les clients n'étaient pas informés de ces utilisations secondaires au moment de l'abonnement, et aucun élément de la preuve ne donnait à penser que ces utilisations étaient liées d'assez près à la création d'un annuaire téléphonique pour que les nouveaux abonnés puissent raisonnablement les considérer comme appropriées. Aucun élément non plus ne tendait à établir que TELUS avait fait un « effort », et encore moins un « effort raisonnable », au sens du principe 4.3.2, pour que les nouveaux abonnés soient informés des fins secondaires de la collecte au moment de celle-ci.

Lorsque les personnes sont convenablement informées des utilisations secondaires potentielles, il reste à savoir quel type de consentement serait approprié en vertu de la LPRPDÉ. Dans certains cas, un consentement négatif peut convenir à des fins secondaires de marketing, mais les conditions suivantes doivent être remplies :

> On doit pouvoir démontrer que les renseignements personnels ne sont pas confidentiels, d'après leur nature et le contexte.
>
> La situation de transmission de renseignements doit être circonscrite et bien définie pour ce qui est de la nature des renseignements personnels utilisés ou communiqués et de l'ampleur de l'utilisation ou de la communication prévue.
>
> Les buts de l'organisme doivent être circonscrits et bien définis, énoncés de manière raisonnablement claire et compréhensible, et mentionnés aux particuliers au moment où l'on recueille leurs renseignements personnels.
>
> L'organisme doit établir une procédure pratique qui permette aux particuliers concernés de retirer leur consentement facilement, de manière peu coûteuse et sur-le-champ, dans le cas où l'on voudrait utiliser leurs renseignements personnels à des fins secondaires; en outre, il doit les aviser de la procédure au moment où il recueille leurs renseignements personnels[94].

Par exemple, le choix du consentement négatif (refus) a été retenu par une entreprise de télécommunication qui a joint à l'envoi de ses relevés de compte mensuels un document qui traitait de ses pratiques relatives à la confidentialité pour le marketing secondaire. L'entreprise offrait aux clients différentes façons simples d'exercer leur

93 *Ibid.*, paragraphe 65. À savoir service d'assistance-annuaire sur Internet, services de base de données – désignés Directory File Service et Basic Listing Interchange File Service – et service CD-ROM.

94 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 192 : Une banque n'obtient pas le consentement explicite de ses clients pour communiquer leurs renseignements personnels – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030723_01_f.asp.

droit de désistement[95]. Les clients pouvaient exercer leur option de refus en appelant à un numéro sans frais, par courriel ou sur le site Web de l'organisation. L'entreprise de télécommunication a indiqué qu'en plus du document envoyé avec les relevés mensuels, elle allait offrir aux clients la possibilité d'exercer leur droit de désistement au moment de l'activation du téléphone. Le Commissariat a considéré cette procédure comme un modèle de consentement négatif.

9.2 Services bancaires

Concernant l'enjeu du consentement négatif à des fins secondaires de marketing, des conclusions opposées ont été formulées dans le cadre d'une enquête où la commissaire adjointe a constaté qu'une banque n'offrait aucune façon d'exercer le droit de désistement en ce qui a trait au matériel promotionnel qui accompagnait le relevé mensuel d'une carte de crédit[96]. La banque refusait qu'une personne se désiste de l'envoi « d'encarts de relevés de compte », à savoir des publicités pour des produits et services. Même si la banque a accepté de cesser le télémarketing et le marketing direct dans le cas du plaignant, elle a fait savoir que, pour cesser l'envoi d'encarts avec les relevés de compte, il lui faudrait intercepter manuellement les relevés dans le cycle de production principale. La banque considérait que cette solution était déraisonnable et qu'aucun renseignement personnel n'était utilisé puisque les encarts étaient insérés dans toutes les enveloppes.

La commissaire adjointe était en désaccord avec la banque; à son avis, la banque utilisait les renseignements personnels du plaignant lorsqu'elle insérait de la publicité dans l'enveloppe contenant le relevé de carte de crédit du plaignant. Cette utilisation était secondaire aux motifs pour lesquels le plaignant avait à l'origine donné son consentement, c'est-à-dire pour recevoir une carte de crédit. Au bout du compte, la commissaire adjointe a conclu que les personnes devaient toujours pouvoir se désister du marketing secondaire et que le refus d'un tel désistement allait à l'encontre des principes 4.3.3 et 4.3.8 de la LPRPDÉ; la banque avait donc contrevenu à la LPRPDÉ, car elle exigeait le consentement à des fins excédant la prestation du service de compte de carte de crédit et elle refusait de donner le droit de retirer le consentement.

Au cours d'une enquête similaire, la commissaire adjointe a exprimé des inquiétudes concernant une pratique de marketing courante dans l'industrie, à savoir envoyer à des détenteurs de carte de crédit des chèques de dépannage non demandés qui contiennent des renseignements personnels, y compris le nom du détenteur, son adresse et son numéro de compte[97]. Ces chèques de dépannage étaient joints aux relevés de compte mensuels des clients et étaient envoyés dans le cadre de diverses promotions ou à la demande des clients. Dans cette affaire, le courrier d'un client, qui contenait des chèques de dépannage,

95 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 207 : Une entreprise de téléphones cellulaires satisfait aux conditions rattachées au consentement négatif – http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_02_f.asp.

96 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 308 : Retrait du consentement à l'insertion d'encarts de promotion dans les relevés de compte – http://www.privcom.gc.ca/cf-dc/2005/308_20050407_f.asp.

97 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 299 : Un voleur encaisse un chèque de dépannage tiré sur un compte de crédit annulé – http://www.privcom.gc.ca/cf-dc/2005/299_050331_03_f.asp#update. Voir la mise à jour à la fin du résumé.

avait été volé, ce qui a permis au voleur de contrefaire un chèque de 900 $ et de l'encaisser. Dans la foulée de ses conclusions, la commissaire adjointe a émis des recommandations selon lesquelles la banque devrait cesser d'envoyer des chèques de dépannage non demandés à ses clients avec les relevés de compte mensuels et plutôt informer les clients de la façon de commander les chèques. La banque a répondu qu'elle ne pouvait pas instaurer un mécanisme de marketing distinct pour les chèques de dépannage en raison des coûts élevés qu'il en résulterait; cependant, elle a accepté de mettre en œuvre des options de consentement négatif et d'améliorer la sécurité des chèques de dépannage.

Dans une autre enquête type, le Commissariat s'est penché sur les pratiques de protection de la vie privée d'une banque qui utilisait et communiquait des renseignements personnels de comptes de carte de crédit à des fins secondaires de marketing[98]. Le Commissariat a constaté que :

- le formulaire de demande de carte de crédit demandait un consentement en très petits caractères au verso;
- le contrat de carte de crédit stipulait que les renseignements qui y figuraient seraient communiqués à des organisations sans préciser lesquelles;
- la demande de carte de crédit en ligne ne contenait pas de lien vers le contrat et ne mentionnait rien au sujet de la communication des renseignements à des tiers;
- la demande de carte de crédit par téléphone comprenait une demande de consentement très générale;
- la politique de protection des renseignements personnels de la banque était plus détaillée, mais elle n'était pas automatiquement distribuée aux clients; ils devaient en faire la demande ou aller sur le site Web de la banque;
- le formulaire de demande et le contrat de carte de crédit mentionnaient que le client pouvait retirer son consentement au marketing secondaire s'il en informait la banque par écrit.

La banque affirmait que les efforts susmentionnés étaient suffisants pour informer les clients et obtenir leur consentement en vertu de la LPRPDÉ. Le Commissariat n'était pas du même avis et a conclu que la banque ne faisait pas d'efforts raisonnables pour informer les personnes des motifs d'utilisation ou de communication des renseignements. Les personnes ne pouvaient pas raisonnablement comprendre à quoi on leur demandait

98 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 83 : Communication alléguée sans consentement de renseignements personnels pour des fins secondaires de marketing par une banque – http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021016_1_f.asp.

de consentir parce que, entre autres, la banque ne leur donnait pas assez d'information à laquelle se référer pour décider de donner ou non leur consentement, la banque utilisait des termes trop vagues et, dans un cas, la banque avait utilisé un jargon juridique et de très petits caractères. La banque n'expliquait pas non plus convenablement que certains services seraient offerts par des tiers à qui elle communiquerait les renseignements personnels des clients.

Le Commissariat a déterminé que la banque enfreignait presque tous les aspects du consentement (principes 4.3, 4.3.2 et 4.3.3) et que ses motifs n'étaient pas appropriés dans les circonstances[99]. En ce qui a trait au consentement négatif, l'incapacité de la banque à offrir « un moyen pratique, immédiat et facile » de refuser qu'elle communique les renseignements personnels à des fins secondaires de marketing ne répondait pas aux attentes raisonnables d'une personne; la banque enfreignait donc également le principe 4.3.5.

9.3 Commerce de détail

Dans une affaire concernant Ticketmaster (entreprise des États-Unis dont la principale activité commerciale est la vente de billets au nom de sites, de promoteurs de spectacles, d'équipes et de ligues sportives pour des évènements qui se tiennent au Canada), une personne s'est plainte que l'entreprise utilisait des renseignements personnels qu'elle recueillait à des fins de marketing pour des tiers, que les clients n'étaient pas informés de façon appropriée de cette pratique et que l'entreprise ne leur offrait pas d'option pratique s'ils ne voulaient pas partager leurs renseignements personnels. La plaignante alléguait que les politiques et les pratiques de l'entreprise concernant la collecte, l'utilisation et la communication des renseignements personnels des clients ne respectaient pas les principes relatifs à la transparence (principes 4.8 et 4.8.1), à l'accès (principes 4.1.4, 4.5, 4.9 et 4.9.3), à la responsabilité (principe 4.1.3) et au consentement (principes 4.3, 4.3.2 et 4.3.3) de l'annexe 1 de la LPRPDÉ.

La commissaire adjointe a déterminé que bien que Ticketmaster ait eu en place une politique de protection des renseignements personnels, celle-ci était longue et complexe; par conséquent, elle ne respectait pas le principe de transparence. La commissaire adjointe a également conclu que la plainte relative au consentement était fondée et réglée. Ticketmaster avait des motifs raisonnables de recueillir les renseignements personnels des clients pour traiter les paiements, acheminer les billets, aviser les clients en cas d'annulation ou de report d'évènements, vérifier l'identité des clients à la prise de possession des billets et remplacer les billets perdus, mais l'entreprise n'avait pas le consentement des clients pour utiliser ces renseignements à des fins de marketing. Le marketing est une fin secondaire et, à ce titre, requiert le consentement pleinement éclairé ou la possibilité de refuser sans pénalité. De plus, la politique initiale de Ticketmaster ne

99 Des lacunes similaires ont mené à des conclusions semblables durant l'enquête visant une entreprise de marketing qui communiquait, à des fins de marketing, les renseignements recueillis dans le cadre de sondages sur des produits grand public. Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 91 : Une entreprise de marketing est accusée de communication inappropriée de renseignements issus d'un sondage – http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021122_f.asp.

précisait pas si des fournisseurs d'évènements utilisaient les renseignements des clients à des fins de marketing et, le cas échéant, de quelle façon ils s'en servaient.

Au cours d'une autre enquête, le commissaire a examiné une plainte contre une organisation qui partageait des renseignements personnels avec ses filiales des autres provinces à des fins secondaires de marketing[100]. Cette enquête portait sur un programme pour acheteurs assidus qui permettait d'accumuler des points à l'achat des produits des commanditaires. L'organisation partageait les renseignements personnels avec ces commanditaires à des fins de marketing. L'inscription au programme d'acheteurs assidus pouvait se faire en personne au moyen d'un formulaire, par téléphone ou en ligne.

Le commissaire a examiné les documents relatifs à la protection des renseignements personnels de l'organisation et a conclu que cette dernière offrait un engagement solennel quant au respect de la vie privée pour les inscriptions en personne ou en ligne. Cet engagement respectait les exigences de la LPRPDÉ, car il précisait clairement les fins de la collecte, de l'utilisation et de la communication des renseignements personnels, y compris les fins de marketing, et les personnes avaient la possibilité de retirer par écrit leur consentement aux fins de marketing. Par contre, en s'inscrivant au programme par téléphone, les personnes n'obtenaient pas les mêmes informations quant aux pratiques de l'organisation en matière de protection de la vie privée – plus particulièrement, on ne leur disait pas que l'utilisation des renseignements personnels à des fins de marketing était facultative ou que le retrait du consentement était possible.

Le commissaire a conclu qu'à l'exception des inscriptions par téléphone, l'organisation avait fait des efforts raisonnables afin d'informer les personnes de l'utilisation et de la communication des renseignements personnels à des fins secondaires de marketing. Leur consentement était donc valide. Toutefois, en exigeant des personnes qu'elles exercent leur droit de désistement par écrit, l'organisation ne leur offrait pas un moyen pratique et immédiat de refuser le consentement aux fins de marketing. Le commissaire a recommandé que l'organisation offre l'accès à une ligne téléphonique sans frais à cet effet.

9.4 Entreprises de transport aérien

Dans une enquête antérieure qui visait Air Canada et Aéroplan, le commissaire a posé d'importantes bases concernant l'enjeu du consentement négatif[101]. Dans cette affaire, Air Canada recueillait, utilisait et communiquait les renseignements personnels des membres du programme Aéroplan à certaines fins. Puis, Air Canada a commencé à partager ces renseignements avec des tiers sans le consentement des personnes concernées. Air Canada a envoyé une notification à seulement 1 p. 100 de ses membres pour leur offrir la possibilité de retirer leur consentement à ce partage.

100 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 78 : Communication alléguée sans consentement de renseignements personnels pour des fins secondaires de marketing par une entreprise – http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021016_6_f.asp.

101 Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 42 (mise à jour) : Air Canada permet à 1 % des membres Aéroplan de se « désister » des pratiques de partage d'information – http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020320_f.asp.

Le commissaire a constaté qu'Air Canada enfreignait la LPRPDÉ de nombreuses manières. Selon lui, l'envoi de la notification à seulement 1 p. 100 des membres était insuffisant. Air Canada se devait de considérer la sensibilité des renseignements pour choisir le consentement approprié. Dans le cadre de cette affaire, les renseignements qui portaient sur les habitudes et les préférences d'achat des membres étaient considérés sensibles et exigeaient par conséquent un consentement positif. Le commissaire a également conclu que les personnes ne pouvaient pas raisonnablement consentir à une fin qui était incompréhensible en raison de son caractère vague et de sa durée indéterminée.

CONCLUSION

Dans ce document, nous avons tenté de présenter aux organisations certaines des leçons apprises au fil de l'expérience pratique que nous avons acquise en interprétant et en appliquant la LPRPDÉ jusqu'à présent. Il s'agit d'un rapport rétrospectif de quelques-uns des enjeux avec lesquels nous avons dû composer, de façon très pratique, au cours des sept premières années de la LPRPDÉ.

Compte tenu de la nouvelle génération de défis qui se profilent à l'horizon, de quoi aura l'air un tel document dans sept ans? Quels genres de nouveaux enjeux en matière de protection de la vie privée la LPRPDÉ devra-t-elle aborder?

Comme la présence des sites de réseaux sociaux, du marketing comportemental, de la technologie sans fil, des systèmes de détection et de surveillance et de la nanotechnologie augmente, nous commençons à peine à distinguer certaines des répercussions que ces technologies émergentes peuvent avoir sur la protection de la vie privée. La mondialisation et la croissance des entreprises en ligne ne feront qu'augmenter la circulation transfrontalière des données. Les pressions constantes en faveur de la sécurité nationale continueront d'infiltrer le secteur privé de manière progressive, mais envahissante, alors que les organisations se voient attribuer des obligations gouvernementales croissantes concernant leur participation aux efforts antiterroristes et policiers. La marchandisation des renseignements personnels et leur valeur croissante ne feront qu'augmenter l'appétit pour de plus en plus de données obtenues par des moyens légaux – et parfois illégaux.

La LPRPDÉ sera-t-elle en mesure de protéger les renseignements personnels dans ce monde en évolution constante? L'examen législatif de la LPRPDÉ, actuellement en cours, est une occasion d'aborder dès maintenant cette question précise. Les gens continueront sans doute à déposer des plaintes au sujet des façons dont ces tendances affectent leurs vies. Ce sont là les situations sous-jacentes que la LPRPDÉ doit traiter, et qu'elle doit certainement redresser. Elles servent d'exemples puissants, démontrant comment les organisations peuvent apprendre de l'expérience des autres afin d'améliorer leurs pratiques de gestion des renseignements personnels pour mieux protéger la vie privée et atténuer les risques inutiles.

Alors que nous tournons la page vers un nouveau chapitre de son histoire, nous attendons avec grand intérêt de voir la LPRPDÉ en action.

TABLEAU DES ENQUÊTES TYPES

Le tableau ci-dessous présente par thèmes les enquêtes types qui ont été citées dans le document. Il comprend des références à la LPRPDÉ, c'est-à-dire aux articles et aux principes les plus pertinents dans le cadre du présent document, et précise les secteurs d'activité concernés.

1. Champ d'application de la Loi			
Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 349	Paragraphe 2(1)	Propriétaires et locataires	Photographie comme renseignement personnel
Résumé de conclusions d'enquête nº 297	Paragraphe 2(1)	Organisations sportives	Courriel d'affaires comme renseignement personnel
Résumé de conclusions d'enquête nº 149	Paragraphe 2(1)	Transport et aéroports	Numéro d'employé comme renseignement personnel
Résumé de conclusions d'enquête nº 25	Paragraphe 2(1)	Diffuseurs	Adresse IP comme renseignement personnel
Résumé de conclusions d'enquête nº 315	Paragraphe 2(1)	Fournisseurs de services de courriel	Adresse IP comme renseignement personnel
Résumé de conclusions d'enquête nº 319	Paragraphe 2(1)	Fournisseurs de services Internet	Adresse IP comme renseignement personnel
BMG Canada Inc. c. John Doe, 2005 CAF 193	Alinéa 7(3)*c*)	Fournisseurs de services Internet	Adresse IP comme renseignement personnel
Gordon c. Canada (Ministre de la Santé), 2008 CF 258	*Loi sur la protection des renseignements personnels* et *Loi sur l'accès à l'information*	Santé	Identification potentielle et renseignements personnels
Résumés de conclusions d'enquête nºs 14 et 15	Paragraphe 2(1)	Santé	Produit du travail
Résumé de conclusions d'enquête nº 303	Paragraphe 2(1)	Immobilier	Produit du travail
Résumé de conclusions d'enquête nº 220	Paragraphe 2(1)	Télémarketing	Produit du travail

Wyndowe c. Rousseau, 2008 CAF 39	Paragraphe 2(1)	Santé et assurance	Produit du travail
Résumé de conclusions d'enquête nº 309	Paragraphe 2(1)	Garderies	Activité commerciale
Résumé de conclusions d'enquête nº 340	Paragraphe 2(1)	Cabinets d'avocats	Activité commerciale
Rodgers c. Calvert, 2004 ON S.C. 22082 (CanLII)	Paragraphe 2(1)	Organismes sans but lucratif	Activité commerciale
Résumé de conclusions d'enquête nº 345	Paragraphe 2(1)	Écoles	Activité commerciale

2. LPRPDÉ à l'étranger

Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 313	Principes 4.1.3 et 4.8	Institutions financières	Impartition à l'étranger
Résumé de conclusions d'enquête nº 333	Principes 4.1.3 et 4.8	Sécurité	Partage de renseignements avec une société mère aux États-Unis
Résumé de conclusions d'enquête nº 365	Principes 4.1.3 et 4.8	Institutions financières	Impartition à l'étranger
Rapport de conclusions (2 avril 2007)	Article 2 et alinéa 7(3) *c*)	Institutions financières	LPRPDÉ et entités étrangères
Lawson c. Accusearch Inc., 2007 CF 125	Articles 2 et 12	Courtiers en données	LPRPDÉ et entités étrangères

3. Surveillance

Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 114	Paragraphe 5(3) et alinéa 7(1)*b*)	Chemins de fer	Surveillance à des fins de sécurité
Eastmond c. Canadien Pacifique Ltée, 2004 CF 852	Paragraphe 5(3) et alinéa 7(1)*b*)	Chemins de fer	Surveillance à des fins de sécurité
Résumé de conclusions d'enquête nº 265	Paragraphe 5(3) et alinéa 7(1)*b*)	Chemins de fer	Surveillance des employés
Résumé de conclusions d'enquête nº 279	Paragraphe 5(3)	Fournisseurs de services Internet	Surveillance des employés
Résumé de conclusions d'enquête nº 264	Paragraphe 5(3)	Chemins de fer	Surveillance des employés et cartes magnétiques
Résumé de conclusions d'enquête nº 290	Paragraphe 5(3) et alinéas 7(2)*a*) et *b*)	Usines de transformation des aliments	Surveillance des employés
Résumé de conclusions d'enquête nº 269	Alinéas 7(1)*b*) et 7(2) *d*)	Secteur industriel	Surveillance des employés et détectives privés

4. Technologies émergentes

Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 281	Paragraphe 5(3) et principes 4.2, 4.3, 4.4 et 4.7	Télécommunications	Empreinte vocale (données biométriques)
Turner c. TELUS Communications Inc., 2005 CF 1601	Paragraphe 5(3) et principes 4.2, 4.3, 4.4 et 4.7	Télécommunications	Empreinte vocale (données biométriques)

Wansink c. TELUS Communications Inc. (C.A.F.) 2007 CAF 21	Paragraphe 5(3) et principes 4.2, 4.3, 4.4 et 4.7	Télécommunications	Empreinte vocale (données biométriques)
Résumé de conclusions d'enquête nº 351	Article 2, paragraphes 5(3), 7(1) et 7(2) et principes 4.2, 4.2.3, 4.3, 4.3.5, 4.3.6, 4.4, 4.5, 4.7 et 4.8	Télécommunications	Systèmes mondiaux de localisation (GPS)

5. Atteintes à la protection des données et mesures de sécurité

Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
TJX Companies Inc./ Winners Merchant International L.P.	Principes 4.2, 4.3, 4.3.3, 4.4 et 4.7	Commerce de détail	Atteinte à la protection des données
Résumé de conclusions d'enquête nº 185	Principe 4.7	Chemins de fer	Mesures de sécurité techniques
Résumé de conclusions d'enquête nº 226	Principe 4.7	Santé	Mesures de sécurité et compétences du personnel
Exemple de plainte réglée en cours d'enquête nº 25	Sans objet	Restaurants	Masquage des renseignements sur les reçus à des fins de sécurité
Résumé de conclusions d'enquête nº 292	Principe 4.7	Entreprises de transport aérien	Authentification et sécurité
Résumé de conclusions d'enquête nº 289	Principe 4.7	Institutions financières	Sécurité et ordinateur portatif volé
Résumé de conclusions d'enquête nº 356	Principe 4.7	Institutions financières	Sécurité et destruction des dossiers

6. Communications négligentes et besoin de formation continue pour les employés

Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 372	Principe 4.7	Télécommunications	Ingénierie sociale et faux-semblant
Breithaupt c. Calm Air (Cour fédérale nº T-2061-04)	Sans objet	Entreprises de transport aérien	Communications négligentes par des employés
Résumé d'incident nº 1	Sans objet	Santé	Télécopies au mauvais destinataire
Résumé d'incident nº 2	Sans objet	Institutions financières	Télécopies au mauvais destinataire
Résumé d'incident nº 3	Sans objet	Institutions financières	Télécopies au mauvais destinataire
Résumé de conclusions d'enquête nº 332	Principes 4.3 et 4.7.1	Institutions financières	Télécopies au mauvais destinataire
Résumé de conclusions d'enquête nº 360	Principes 4.3 et 4.7.1	Institutions financières	Courriels au mauvais destinataire
Résumé de conclusions d'enquête nº 242	Principe 4.7	Transport	Compétences et formation du personnel concernant les renseignements sensibles
Résumé de conclusions d'enquête nº 54	Principe 4.7	Télécommunications	Formation du personnel concernant la confidentialité

Résumé de conclusions d'enquête nº 344	Principe 4.7	Institutions financières	Communications négligentes par des employés
Résumé de conclusions d'enquête nº 200	Principe 4.3	Institutions financières	Communications négligentes par des employés
Exemple de plainte réglée en cours d'enquête nº 27	Sans objet	Santé	Communications négligentes par des employés
Résumé de conclusions d'enquête nº 270	Alinéa 7(3)*b*) et principe 4.3	Institutions financières	Communications négligentes par un système automatisé
Résumé de conclusions d'enquête nº 154	Principe 4.7	Institutions financières	Documents de prêt hypothécaire postés dans une enveloppe non scellée

7. Collecte excessive de renseignements

Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 361	Paragraphe 5(3) et principes 4.3.3 et 4.4	Commerce de détail	Pièce d'identité avec photo pour des retours et des échanges
Résumé de conclusions d'enquête nº 169	Principes 4.3.3 et 4.4	Institutions financières	Renseignements pour ouvrir des comptes
Exemple de plainte réglée en cours d'enquête nº 28	Sans objet	Commerce de détail	Pièce d'identité avec photo pour ouvrir un compte
Exemple de plainte réglée en cours d'enquête nº 19	Sans objet	Propriétaires et locataires	NAS pour louer un appartement
Résumé de conclusions d'enquête nº 22	Paragraphe 5(3) et principes 4.3.3 et 4.4.1	Télécommunications	NAS pour une connexion Internet
Résumé de conclusions d'enquête nº 280	Paragraphe 5(3) et principe 4.3.3	Télécommunications	Pièce d'identité avec photo pour l'achat d'équipement
Résumé de conclusions d'enquête nº 368	Principes 4.3.3 et 4.4.1	Assurance	Collecte à partir d'un formulaire d'assurance
Résumé de conclusions d'enquête nº 257	Principe 4.4	Transport	Certificats pour congé de maladie
Résumé de conclusions d'enquête nº 233	Principe 4.4	Transport	Certificats pour congé de maladie
Résumé de conclusions d'enquête nº 135	Paragraphe 5(3) et principe 4.4	Transport	Certificats pour congé de maladie
Résumé de conclusions d'enquête nº 235	Principe 4.3	Transport	Vérification au centre hospitalier au sujet des examens médicaux d'un employé

8. Meilleur accès aux renseignements personnels			
Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Résumé de conclusions d'enquête nº 367	Article 8 et principe 4.9	Cabinets d'avocats	Accès
Vanderbeke c. Banque Royale du Canada, 2006 CF 651	Principe 4.9	Institutions financières	Type d'accès
Résumé de conclusions d'enquête nº 352	Articles 8, 9 et principe 4.9	Entreprises de transport aérien	Accès et action en justice
Résumé de conclusions d'enquête nº 285	Articles 8 et 9 et principes 4.9 et 4.9.4	Non disponible	Accès, action en justice et droits pour l'accès
Résumé de conclusions d'enquête nº 306	Alinéas 9(3)*a*) et 9(3) *d*) et principe 4.9	Santé	Accès, action en justice et privilège
Rousseau c. Wyndowe, 2006 CF 1312	Alinéas 9(3)*a*) et 9(3) *d*) et principe 4.9	Santé	Accès, action en justice et privilège
Résumé de conclusions d'enquête nº 283	Principe 4.9.4	Institutions financières	Droits pour l'accès
Résumé de conclusions d'enquête nº 354	Alinéas 8(6)*a*) et 8(6) *b*), principes 4.9 et 4.9.4	Non disponible	Droits pour l'accès
Résumé de conclusions d'enquête nº 328	Principe 4.9.4	Santé	Droits pour l'accès
9. Fins secondaires de marketing			
Affaire	LPRPDÉ	*Secteur d'activité*	*Enjeu*
Englander c. TELUS Communications Inc., 2004 CAF 387	Paragraphe 5(3), principes 4.2 et 4.3	Télécommunications	Consentement
Résumé de conclusions d'enquête nº 42	Paragraphe 5(3) et principes 4.2 et 4.3	Entreprises de transport aérien	Consentement
Résumé de conclusions d'enquête nº 207	Principe 4.3	Télécommunications	Consentement négatif
Résumé de conclusions d'enquête nº 192	Principe 4.3	Institutions financières	Consentement
Résumé de conclusions d'enquête nº 308	Principes 4.3.3 et 4.3.8	Institutions financières	Consentement négatif
Résumé de conclusions d'enquête nº 299	Principe 4.7.1	Institutions financières	Mesures de sécurité relatives au marketing secondaire
Résumé de conclusions d'enquête nº 78	Principes 4.2.3 et 4.3	Programmes d'acheteurs assidus	Consentement négatif
Résumé de conclusions d'enquête nº 83	Paragraphe 5(3) et principe 4.3	Institutions financières	Consentement
Résumé de conclusions d'enquête nº 91	Principes 4.2.3 et 4.3	Entreprises de marketing	Consentement