L'évocation du nom « TJX » est sans aucun doute très convaincante lorsque des experts en matière de sécurité demandent aux cadres supérieurs des fonds pour mettre à niveau le système de sécurité.

Toutes les organisations doivent recourir à un système de sécurité solide pour protéger les renseignements personnels. Dire en guise d'excuse que « Nous n'étions pas plus lents que les autres compagnies » ne suffit pas.

Les mesures de sécurité efficaces coûtent cher, mais beaucoup moins que la réparation des dégâts par suite d'une fuite de données majeure. Selon les experts en matière de sécurité, les atteintes importantes à la sécurité des données coûtent plusieurs fois le coût de l'installation de sauvegardes adéquates dès le départ.

De bonnes pratiques en matière de protection de la vie privée sont également très efficaces pour protéger les renseignements personnels.

La *LPRPDÉ* énonce dix principes relatifs à l'équité dans le traitement des renseignements que doivent suivre les entreprises. Ces principes – parfois appelés « règles d'or » de la protection de la vie privée – incluent des éléments fondamentaux tels que l'obtention du consentement pour l'utilisation des renseignements personnels; la limitation de l'utilisation, de la communication et de la conservation des renseignements personnels; et l'utilisation de mesures de sécurité appropriées.

Le point de départ de la mise en œuvre de ces principes est l'examen objectif des renseignements personnels recueillis. Les organisations ne devraient recueillir que les renseignements personnels absolument essentiels. Après tout, si vous ne disposez pas de ce type d'information, vous ne pouvez le perdre ou vous le faire voler.

La seconde étape cruciale consiste à reconnaître la valeur des renseignements personnels recueillis et à les protéger adéquatement.

En suivant ce conseil de base, une organisation devrait se retrouver avec un objectif de collecte des données relativement petit et bien protégé.

Le CPVP a élaboré une formation en ligne plus détaillée sur la manière dont les détaillants peuvent mettre en pratique les principes relatifs à l'équité dans le traitement des renseignements personnels. Le cours est offert sur notre site Web.

La formation des employés est également cruciale pour prévenir les fuites de données. Dans bon nombre de rapports que nous avons reçus des entreprises, la cause de l'atteinte à la sécurité des données était le défaut d'un employé de respecter les procédures de la compagnie.

À titre d'exemple, le vol d'ordinateur portatif est un type courant d'atteinte à la sécurité des données. Des employés quittent le bureau avec des ordinateurs portatifs contenant des renseignements personnels délicats sur les clients – ce qui est contraire aux politiques de l'entreprise en matière de sécurité.

L'efficacité des politiques et des procédures dépend de la qualité de la formation qui vise à raffermir leur application.

Malheureusement, un sondage mené en 2007 auprès des entreprises canadiennes pour le Commissariat a révélé que seulement le tiers d'entre elles avaient formé leur personnel à l'égard de leurs responsabilités découlant des lois canadiennes en matière de protection des renseignements personnels. Les grandes entreprises étaient les plus susceptibles d'avoir offert une formation, comme l'indiquaient 63 p. 100 d'entre elles.

Les entreprises n'ayant donné aucune formation aux employés qui gèrent les renseignements personnels s'exposent à des risques beaucoup plus grands d'atteinte à la sécurité des données. Nous espérons que les résultats seront plus encourageants la prochaine fois que nous mènerons un sondage sur la conformité à la *LPRPDÉ*.

Au cours de 2007, nous avons élaboré des directives concernant les atteintes à la sécurité des données, en consultation avec l'industrie et des groupes de la société civile. Ces directives énoncent les principales étapes que devraient suivre les organisations victimes d'un accès non autorisé, comme contenir l'atteinte, évaluer les risques connexes, informer les personnes touchées et prévenir les fuites futures. La Nouvelle-Zélande a également adopté ces directives comme modèle à suivre et la commissaire à la protection de la vie privée de l'Australie se propose de faire de même.

Nous avons clairement indiqué que les directives facultatives n'éliminaient pas la nécessité d'avoir une loi prévoyant la notification des atteintes à la sécurité des données.

En fait, nous avons exhorté le gouvernement fédéral à modifier la *LPRPDÉ* afin d'y ajouter une disposition sur la notification des atteintes à la sécurité des données.

Nous sommes d'avis qu'une notification obligatoire aiderait à protéger les renseignements personnels de deux manières très importantes. Premièrement, cela encouragerait les organisations à prendre plus au sérieux la protection de la vie privée et la sécurité. Deuxièmement, les gens disposeraient de l'information voulue pour prendre des mesures afin de se protéger eux-mêmes contre le vol d'identité ou d'autres formes de fraude.

Il ne fait pas de doute que les gens désirent ce genre d'information.

Plus des trois quarts des Canadiennes et Canadiens (77 p. 100) croient qu'il faudrait avertir les organismes gouvernementaux et les personnes touchées lorsque des renseignements personnels délicats sont compromis par suite d'une atteinte à la sécurité des données, selon un sondage commandé en 2007 par le Commissariat. Entre-temps, 66 p. 100 souhaitaient être avisés dans le cas de compromission de renseignements non délicats.

Selon un des principes de la *LPRPDÉ*, les gens devraient avoir prise sur leurs renseignements personnels. La notification des atteintes à la sécurité des données donne un choix aux gens. Ainsi, ils peuvent décider par eux-mêmes de la manière de réagir à une telle atteinte, en décidant par exemple que ce serait une bonne idée de vérifier plus souvent leurs rapports de crédit, ou encore qu'aucune mesure n'est justifiée.

Ce qui compte, c'est que la personne ait prise sur ses renseignements personnels.

Le Commissariat croit que l'envoi d'une notification est un élément important d'une approche globale pour réduire les atteintes à la sécurité des données.

La débâcle de TJX, en plus des manchettes concernant les disques informatiques et disques durs manquants ainsi que d'autres données perdues, constitue un avertissement pour toutes les organisations qui recueillent des renseignements personnels. Ces incidents illustrent de façon frappante à quel point il est important que les entreprises accordent la priorité à la protection de la vie privée et à la sécurité.

Lorsque les Canadiennes et Canadiens confient leurs renseignements personnels à une organisation, ils s'attendent à ce que ces renseignements soient bien protégés – ce que la loi exige d'ailleurs.

ENQUÊTE SUR UNE ATTEINTE À LA SÉCURITÉ DES DONNÉES

L'AFFAIRE TJX : COMMENT DES PIRATES ONT PU ACCÉDER À 94 MILLIONS DE CARTES DE CRÉDIT ET DE DÉBIT

Ce qu'on a décrit comme étant le plus grand vol en ligne jamais réalisé a commencé un jour d'été de 2005.

On croit que les voleurs, armés d'une antenne, d'un ordinateur portatif et de quelques logiciels spécialisés, se sont retrouvés à l'extérieur d'un magasin Marshall's à Miami et ont fait irruption dans les réseaux locaux sans fil et faiblement protégés du magasin.

Une fois à l'intérieur, ils ont utilisé les serveurs informatiques qui traitent et stockent les renseignements sur les clients obtenus lors de transactions effectuées pour des centaines de magasins appartenant à TJX, ce géant de la vente au détail à marge réduite, y compris Winners et HomeSense au Canada.

Pendant un an et demi, les voleurs ont pillé le système informatique de TJX.

Au bout du compte, ils auront accédé à au moins 94 millions de cartes de crédit et de débit ainsi qu'aux noms, adresses et numéros de permis de conduire de gens qui avaient rapporté de la marchandise dans les magasins de TJX.

Il ne s'agissait pas d'un crime particulièrement compliqué. On trouve facilement sur Internet des instructions détaillées sur la manière de déchiffrer le protocole cryptographique servant à protéger les réseaux sans fil de TJX.

C'est un fait bien établi depuis un certain temps que ce protocole cryptographique – le système WEP (Wired Equivalent Privacy, ce qui signifie confidentialité équivalente aux transmissions par fil) – ne protégeait pas adéquatement le réseau puisqu'une personne possédant un peu de savoir-faire en informatique pouvait facilement le contourner.

TJX était au fait des préoccupations entourant son protocole cryptographique et était en voie de se convertir à une technologie plus fiable au moment où est survenu l'accès non autorisé. Selon nous, la conversion ne s'est pas faite dans un délai raisonnable.

L'enquête du CPVP, réalisée de concert avec le commissaire à l'information et à la protection de la vie privée de l'Alberta, Frank Work, a mené à la conclusion que TJX ne s'était pas conformée aux lois fédérales et albertaines sur la protection des renseignements personnels.

DE LOURDES DÉFAILLANCES

L'enquête a mis en lumière quelques défaillances critiques :

1. TJX recueillait trop de renseignements et les conservait beaucoup trop longtemps.

L'entreprise n'aurait pas dû recueillir les numéros de permis de conduire et autres numéros d'identification lors des retours de marchandise sans reçu. Un permis de conduire est la preuve qu'une personne est autorisée à conduire une auto – non pas un identificateur servant à analyser les habitudes concernant les retours de marchandise. En outre, un numéro de permis de conduire est inutile pour identifier des voleurs.

En réponse à nos préoccupations, TJX a proposé un nouveau processus novateur pour prévenir les retours de marchandise frauduleux. L'entreprise continuera de recueillir et introduire dans le système de terminaux des points de vente des renseignements tels que le numéro du permis de conduire. Toutefois, le numéro sera instantanément converti en un numéro d'identification unique, permettant ainsi de faire le suivi des retours de marchandise non accompagnée d'un reçu sans conserver les numéros d'identification originaux.

Avant l'affaire de l'accès non autorisé, les renseignements d'identification recueillis auprès des personnes rapportant de la marchandise étaient conservés indéfiniment.

L'entreprise conservait également pendant longtemps les données relatives aux cartes de crédit. En fait, certains des renseignements volés impliquaient des transactions qui remontaient à plusieurs années.

2. TJX a négligé de mettre à jour en temps opportun ses systèmes de sécurité.

Il a fallu deux années à TJX pour réaliser une conversion vers un protocole cryptographique à jour. C'est durant cette période que se sont produites les atteintes à la sécurité des données. Par conséquent, l'entreprise n'a pas respecté les exigences en matière de normes de sécurité des données décrétées par l'industrie des cartes de paiement.

3. TJX n'a pas surveillé adéquatement son système, ce qui l'a empêchée de déceler les signes d'une intrusion.

Les voleurs ont été en mesure de poursuivre le vol de données pendant une année et demie avant que TJX n'apprenne la présence de logiciels douteux dans une partie de son système informatique. En appliquant des mesures de contrôle adéquates, TJX aurait découvert cet incident plus tôt.

PRÉPARER L'AVENIR

La société TJX s'est conformée à toutes les recommandations du CPVP visant à améliorer la sécurité, le contrôle et d'autres enjeux entourant la gestion des renseignements personnels.

Un an après qu'on l'a mise au jour, la fuite engendre encore des répercussions.

L'entreprise continue de répondre à certaines poursuites engagées contre elle. La Federal Trade Commission des États-Unis poursuit son enquête à l'instar du secrétaire à la Justice du Massachusetts au nom d'un groupe de plus de 30 secrétaires à la Justice d'États.

On ignore combien la fuite coûtera ultimement à l'entreprise – mais le total se chiffrera certainement en centaines de millions de dollars.

Avant la fin de 2007, TJX avait désigné un chef de la protection des renseignements personnels et recherchait un directeur de la protection de la vie privée pour élaborer et mettre en œuvre un programme complet de sécurité et de protection de la confidentialité des renseignements personnels.

Manière dont le Commissariat aide les organisations à prévenir les atteintes à la sécurité des données

- Nous avons lancé un outil d'apprentissage en ligne qui offre aux détaillants un guide contenant les étapes à suivre pour protéger les renseignements personnels des clients et répondre aux obligations de la *LPRPDÉ*.
- Nous avons publié divers documents électroniques et imprimés sur la manière dont les entreprises peuvent sauvegarder des renseignements personnels, y compris la brochure intitulée « Protection des renseignements personnels : vos responsabilités – Guide à l'intention des entreprises et des organisations ».
- De concert avec des groupes industriels et des groupes de défense des consommateurs, nous avons élaboré des lignes directrices d'application volontaire concernant les atteintes à la sécurité des données.
- Nous conseillons et épaulons les organisations qui prennent des mesures en réaction à des atteintes à la sécurité des données, notamment en donnant des conseils sur les notifications à fournir aux personnes touchées par ce problème.
- Nous continuons à faire pression sur le gouvernement fédéral pour qu'il rende obligatoire les notifications d'atteintes à la sécurité des données en vertu de la *LPRPDÉ*, ce qui, selon nous, encouragerait les entreprises à améliorer leurs mesures de sécurité.
- Nous vérifions la façon dont les organisations visées par la *LPRPDÉ* gèrent les renseignements personnels lorsque nous avons des motifs raisonnables de croire qu'une organisation enfreint la loi.
- Nos enquêtes sur les plaintes concernant la vie privée aident à cerner les mesures que peuvent prendre les entreprises pour mieux protéger les renseignements personnels.

AMÉLIORATION DE LA *LPRPDÉ* : UN EXAMEN DE NOTRE LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS À L'INTENTION DU SECTEUR PRIVÉ

Un comité parlementaire a réalisé un examen obligatoire de la* LPRPDÉ *en 2007 – une étape importante pour raffermir les mesures de protection de la vie privée des Canadiennes et Canadiens

La *LPRPDÉ*, ainsi que son pendant pour le secteur public, la *Loi sur la protection des renseignements personnels*, de même que les lois provinciales relatives à la protection de la vie privée, fournissent l'assise de la protection de la vie privée au Canada.

Le paysage de la protection de la vie privée change constamment – et nos lois doivent suivre le rythme.

On n'a qu'à songer à la profondeur des changements survenus dans le monde depuis dix ans, alors que nous commencions à parler de ce à quoi devait ressembler une loi sur la protection de la vie privée dans le secteur privé au Canada.

À l'époque, le terme « inforoute » se voulait accrocheur. Aujourd'hui, c'est une réalité. Le mince filet de renseignements personnels traversant les frontières s'est transformé en torrent. Dans l'intervalle, de nouvelles technologies telles que les dispositifs de repérage soumettent la protection de la vie privée à de nouveaux périls. Et les conséquences du 11 septembre font en sorte que les gouvernements demandent aux entreprises davantage de renseignements sur nos vies au quotidien.

Il est crucial que la *LPRPDÉ* puisse continuer à répondre à tous ces nouveaux défis. La *Loi sur la protection des renseignements personnels*, qui est désespérément dépassée – elle n'a pas changé en 25 ans – est la preuve qu'il est dangereux de négliger de moderniser les lois sur la protection des renseignements personnels.

Heureusement, les concepteurs de la *LPRPDÉ* ont reconnu l'importance de procéder à des mises à jour régulières. Ainsi, le Parlement est tenu de réviser tous les cinq ans la partie de cette loi qui porte sur la protection des données.

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a pris en charge le premier travail de révision quinquennale. Ses activités en ce sens ont débuté durant l'été 2006.

En février 2007, les membres du Comité ont conclu les audiences publiques qui ont porté sur un éventail d'enjeux. Ils ont entendu 67 témoins et pris en considération 34 mémoires de la part de particuliers, d'associations du secteur privé, de défenseurs du droit à la vie privée et de la commissaire à la protection de la vie privée.

Dans l'ensemble, nous avons le sentiment que la Loi a été bien accueillie, qu'elle fonctionne raisonnablement bien et que nous disposons de la plupart des outils et des pouvoirs voulus pour la faire appliquer. La Loi offre à la population canadienne de solides protections de la vie privée dans la sphère commerciale.

Dans nos présentations au Comité, nous avons indiqué que la loi n'est pleinement en vigueur que depuis 2004. Bien que l'expérience acquise à ce jour ait été instructive, il faut plus de temps avant que ne surviennent des changements d'envergure et que ne se fassent sentir toutes les répercussions d'une loi complexe.

Cela dit, certains ajustements seraient souhaitables pour s'assurer que les mesures de protection de la vie privée évoluent au même rythme que les nouvelles tendances et technologies.

En mai 2007, le Comité a présenté son rapport final, qui incluait 25 recommandations aux fins d'examen par le gouvernement ou de discussions.

Les modifications suggérées touchaient un grand nombre d'enjeux, dont les suivants : renseignements sur les personnes-ressources du monde des affaires; renseignements sur le produit du travail, tels que les habitudes de prescription des médecins; relations employé-employeur; organismes d'enquête; déclarations des témoins; application de la loi et sécurité nationale; exceptions pour la personne ou la famille; communication des renseignements personnels avant le transfert d'entreprises; mesures de protection supplémentaires pour les mineurs; notification obligatoire des atteintes à la sécurité des données.

Nous sommes profondément reconnaissants des efforts des parlementaires, chercheurs, organisations et citoyens qui ont mis leur expérience et leurs compétences au profit du processus d'examen.

Le gouvernement du Canada a déposé sa réponse en octobre. Selon nous, l'un des éléments très importants de la réponse concernait la reconnaissance du fait que les menaces à la protection de la vie privée font de plus en plus appel à des mesures d'envergure internationale. L'industrie du traitement des données s'internationalise toujours plus, tout comme le font les risques posés à la sécurité des données.

La coopération intergouvernementale, le partage de renseignements entre les administrations et l'attention accordée aux tendances qui se dessinent dans d'autres parties du monde sont tous devenus des considérations stratégiques cruciales alors que nous travaillons à protéger la vie privée des Canadiennes et Canadiens.

En octobre, Industrie Canada a présenté un avis de consultation pour obtenir l'opinion du public quant à la meilleure manière de mettre en œuvre certaines dispositions de la réponse gouvernementale. On a accordé une importance particulière aux points de vue sur les dispositions relatives à la notification des atteintes à la sécurité des données, et aux concepts de « produit du travail » et d'« autorité légitime ». En outre, Industrie Canada a cherché à obtenir des opinions sur les déclarations des témoins, le consentement des mineurs et les organismes d'enquête.

Dans le cadre de cette série de consultations, la commissaire à la protection de la vie privée a demandé au ministre de l'Industrie d'examiner étroitement cinq enjeux qui auront une incidence marquée sur notre travail dans les années à venir :

- Nous avons continué de promouvoir une approche « contextuelle » en ce qui touche l'information sur le produit du travail.

- Nous avons plaidé en faveur d'une notification obligatoire des atteintes à la sécurité des données, et insisté sur la nécessité d'établir clairement des déclencheurs et des seuils dans toute nouvelle disposition de la *LPRPDÉ*.

- Nous avons demandé à ce que demeurent ouvertes les modifications possibles à la *LPRPDÉ* concernant l'accès aux documents visés par le secret professionnel qui lie un avocat à son client, en attendant une décision de la Cour suprême du Canada dans l'affaire de la *Commissaire à la protection de la vie privée du Canada c. Blood Tribe Department of Health*.

- Nous avons insisté pour que toute nouvelle disposition sur la protection de la vie privée dans le contexte de la relation employeur-employé prenne en considération les lois de l'Alberta et du Québec afin de mieux reconnaître le fait que l'inégalité du pouvoir de négociation dans les relations de travail implique que les employés pourraient ne pas se sentir en position de refuser de consentir à la collecte de leurs renseignements personnels. Le CPVP voit l'avantage de l'approche albertaine

d'un code relatif aux employés reposant sur le critère des fins raisonnables, en combinaison avec la notion du Code civil du Québec qui oblige les employeurs à respecter la dignité des travailleurs.

- Nous avons demandé davantage de latitude pour refuser et/ou abandonner des plaintes si leur enquête ne répond à aucun but utile ou ne sert pas l'intérêt public, ce qui nous permettrait alors de concentrer nos ressources d'enquête sur des questions d'un intérêt systémique plus vaste.

La date limite pour faire parvenir des observations à Industrie Canada était la mi-janvier 2008. Le ministère a reçu 67 mémoires et en faisait l'examen au début de 2008.

Nous sommes impatients de passer à la prochaine étape de l'examen de la Loi et à l'important dialogue qu'il engendre entre les défenseurs du droit à la vie privée, les organes de réglementation, l'industrie et les parlementaires.

ENQUÊTES SUR LES PLAINTES ET DEMANDES DE RENSEIGNEMENTS

Les Canadiennes et Canadiens étant davantage au fait des enjeux relatifs à la protection de la vie privée, les organisations doivent faire en sorte de s'acquitter de leurs responsabilités concernant les renseignements personnels. De façon plus particulière, les consommateurs connaissent de mieux en mieux les graves ramifications du vol d'identité, ce qui les amène à insister davantage auprès des entreprises pour qu'elles respectent leurs obligations lorsqu'elles recueillent des renseignements personnels.

Les gens ne souhaitent pas que de l'information de nature délicate telle que leur numéro de permis de conduire soit recueillie et conservée sans raison légitime, tout comme ils ne veulent pas que le numéro de leurs cartes de crédit et les dates d'expiration soient imprimés sur les reçus.

Bon nombre d'entreprises prennent au sérieux leurs responsabilités en matière de protection de la vie privée. Par contre, il ne fait pas de doute – d'après les plaintes reçues et les atteintes à la sécurité des données volontairement déclarées au Commissariat – qu'une grande quantité d'organisations pourraient en faire davantage.

Les entreprises qui manipulent les renseignements personnels doivent régulièrement mettre à jour leurs politiques et pratiques en matière de protection de la vie privée. Elles doivent tenir à jour leur système de sécurité des données. De plus, il leur faut veiller à ce que les employés soient informés des changements et reçoivent une formation régulière.

Demandes de renseignements

La Section des demandes de renseignements répond aux questions des Canadiennes et Canadiens, des institutions gouvernementales, des organisations du secteur privé et du milieu juridique. Les agents responsables des demandes de renseignements fournissent de l'information sur un vaste éventail d'enjeux en vertu de la *LPRPDÉ* et de la *Loi sur la protection des renseignements personnels*.

En 2007, nous avons reçu 7 636 demandes reliées à la *LPRPDÉ*, ce qui représente une augmentation appréciable par rapport aux 6 050 demandes reçues l'année précédente. Nous avons constaté une hausse marquée de l'intérêt envers le vol d'identité et les sites de réseautage social comme Facebook.

Plaintes

En 2007, nous avons reçu 350 nouvelles plaintes en vertu de la *LPRPDÉ*. Ainsi, nous en avions reçu 424 en 2006, 400 en 2005 et 723 en 2004.

Cette diminution d'une année à l'autre s'explique en partie par le processus simplifié d'acceptation des plaintes mis en place en 2007. Selon ce processus, lorsqu'une personne formule une plainte qui est, dans les faits, similaire à d'autres plaintes déjà sous enquête, nous informons cette personne que la question est déjà sous enquête et sera prise en compte par la commissaire dans ses conclusions. Cette approche est également utilisée dans le cas des plaintes pour lesquelles nous avons déjà tiré des conclusions dans une cause similaire.

Dans de tels cas, nous offrons aux plaignants la possibilité d'invoquer des conclusions similaires afin de résoudre les problèmes particuliers qu'ils peuvent avoir avec une organisation.

Par exemple, nous poursuivons présentement cinq enquêtes concernant le dépistage des drogues dans le cadre d'un emploi. Dans les circonstances, 27 autres personnes ont accepté de ne pas déposer de plainte officielle ayant trait au même enjeu.

NOTE : On trouvera de l'information détaillée sur les plaintes de même que des conclusions et autres décisions dans l'annexe 1 du présent rapport.

Dans certains cas, bien que la situation d'une personne soit similaire à celle d'une autre qui a porté plainte, les faits peuvent être suffisamment différents pour justifier une enquête complète.

Une autre cause possible de la baisse du nombre de plaintes est que les organisations connaissent peut-être mieux leurs obligations liées à la protection de la vie privée. De plus, bon nombre d'entre elles disposent maintenant de processus internes de résolution des plaintes afin de régler avec leurs clients les questions de protection de la vie privée. La Section des demandes de renseignements conseille également aux gens de chercher à régler leurs différends avec les organisations avant de déposer une plainte officielle au Commissariat.

Plaintes par secteur

Comme c'est le cas depuis 2004, moment de la mise en œuvre intégrale de la *LPRPDÉ*, le secteur des institutions financières a été, en 2007, le plus souvent ciblé par les plaintes. Nous avons reçu 105 plaintes impliquant des institutions financières en 2007, ce qui représente près du tiers de toutes les plaintes formulées en vertu de la *LPRPDÉ*. Cette proportion est similaire à celle observée ces dernières années.

À l'image des années précédentes, les autres principaux secteurs de plaintes ont été les télécommunications, les assurances, les ventes et le transport. Toutefois, au cours des dernières années, nous avons constaté une diminution des plaintes impliquant des entreprises dans ces secteurs.

Nous avons enregistré une hausse régulière des plaintes concernant les services professionnels et les services d'hébergement. Toutefois, le nombre de plaintes contre ces secteurs demeure faible en comparaison des autres.

En ce qui concerne les plaintes impliquant l'industrie de l'assurance, on constate un nombre accru de dossiers où il est question de collecte clandestine de renseignements personnels par des firmes d'enquêteurs privés.

La *LPRPDÉ* comporte des dispositions où une compagnie d'enquête privée est désignée comme un « organisme d'enquête du secteur privé » qui assume des responsabilités précises en vertu de la Loi.

Nous comprenons l'éventuel besoin d'une collecte clandestine de renseignements personnels là où ont échoué d'autres efforts moins envahissants pour la vie privée. Cependant, ce type d'enquête soulève une grande préoccupation en raison du risque que des tiers innocents puissent être filmés en secret par des caméras de surveillance vidéo. Peu d'entre nous aimeraient être enregistrés sur vidéo en robe de chambre sur notre perron avant simplement parce que nous sommes voisins d'une personne soupçonnée de fraude à l'endroit d'une compagnie d'assurance.

Nous travaillons avec des sociétés d'assurance et des organismes d'enquête privée afin de trouver un équilibre entre leur besoin de mener leurs affaires et le droit des gens à leur vie privée. Les compagnies d'assurance et leurs sous-traitants devraient utiliser la surveillance clandestine en dernier recours seulement. Les entreprises devraient s'assurer que la décision d'effectuer de la surveillance clandestine provient de la haute direction.

Une partie de la solution pourrait être que les compagnies d'assurance établissent des contrats détaillés avec les organismes d'enquête où seraient clairement définis les

paramètres de la surveillance. En outre, ces organismes doivent élaborer des politiques précises concernant la surveillance, y compris l'enregistrement de tiers sur vidéo.

Tendances au chapitre des plaintes

Nous avons résolu 420 plaintes en 2007. La grande majorité d'entre elles (39 p. 100) concernait des questions d'utilisation et de communication de renseignements personnels, une tendance observée ces dernières années. À l'image des années précédentes, d'autres types courants de plaintes avaient trait à la collecte (19 p. 100) et à l'accès (16 p. 100).

Près du tiers (30 p. 100) des plaintes résolues en 2007 ont été réglées en cours d'enquête. Il s'agit de plaintes pour lesquelles le Commissariat a négocié un résultat satisfaisant pour toutes les parties, sans avoir eu à émettre de conclusions. En 2004, nous avons défini la catégorie « réglée en cours d'enquête » afin de faire le suivi de ce résultat.

Plaintes résolues en 2007 – Par conclusions

	Pourcentage
Réglées en cours d'enquête	30
Abandonnées	21
Non fondées	15
Fondées et résolues	15
Résolues	10
Réglées rapidement	3
Hors juridiction	3
Fondées	2

En 2004, 40 p. 100 de nos cas ont été réglés en cours d'enquête. Toutefois, ce pourcentage a, par la suite, diminué de façon constante. Cette tendance témoigne peut-être du fait que nous nous attaquons à des cas plus complexes nécessitant une enquête approfondie.

Un nombre appréciable de dossiers résolus ont été abandonnés en raison d'un désistement (21 p. 100) du plaignant ou du Commissariat. Cette donnée représente une hausse par rapport aux années précédentes. Comme ce fut le cas antérieurement, certains plaignants ont décidé pour des raisons personnelles d'abandonner leur plainte. D'autres n'ont pas poursuivi l'affaire parce qu'ils en sont arrivés à une entente avec l'organisation avant le début de l'enquête. D'autres, enfin, laissent tomber leur plainte à cause des délais de traitement prolongés. Parfois, le Commissariat doit abandonner des plaintes parce que les plaignants ne lui ont pas fourni les détails additionnels qu'il leur avait demandés et qui étaient nécessaires pour réaliser l'enquête.

Une fois les enquêtes complétées, 15 p. 100 des plaintes se sont révélées non fondées alors que les organisations s'étaient conformées à la *LPRPDÉ*. Une autre proportion de 15 p. 100 des plaintes étaient fondées et ont été résolues. En d'autres mots, il

y avait violation de la *LPRPDÉ*, mais la partie intimée a accepté d'appliquer nos recommandations.

On dira d'une plainte ayant fait l'objet d'une enquête complète qu'elle est soit fondée, soit fondée et résolue, selon le niveau de coopération reçue de la partie intimée.

Une plainte est considérée comme fondée lorsque la commissaire est d'avis qu'il y a vraisemblablement eu violation de la *LPRPDÉ*. Elle prépare un rapport préliminaire assorti de recommandations concernant des mesures correctives que devrait appliquer la partie intimée, qui a 30 jours pour répondre à ce rapport.

Ce processus de rapport préliminaire établi en 2006 s'est révélé un moyen efficace de s'assurer que les organisations demeurent responsables.

Si la partie intimée se conforme aux recommandations, on parle habituellement d'une plainte fondée et résolue. Dans les cas où la partie intimée ne se conforme pas intégralement, la plainte est considérée comme étant fondée.

En 2007, nous avons produit des rapports préliminaires pour 38 plaintes résolues. De ce nombre, 34 organisations se sont conformées aux recommandations de la commissaire.

En 2007, seulement quatre organisations ont choisi de ne pas mettre en œuvre nos recommandations au terme de l'enquête. Dans de tels cas, la commissaire a de façon constante cherché à faire confirmer ses recommandations par la Cour fédérale.

Au moment où nous nous préparions à publier ce rapport annuel, les quatre organisations qui avaient initialement refusé d'adopter nos recommandations avaient finalement accepté de se conformer, soit avant ou après que nous ayons renvoyé les causes au contentieux.

Délais de traitement

Le délai de traitement moyen (calculé à partir de la date où la plainte est reçue jusqu'à la date où le rapport des conclusions est mis à la poste) des plaintes en vertu de la *LPRPDÉ* résolues en 2007 était de 15,7 mois – à peu près le même qu'en 2006.

Fait plus positif, seulement 44 dossiers étaient en suspens – non attribués parce qu'aucun enquêteur n'est disponible – à la fin de 2007. C'est beaucoup plus bas que les 76 dossiers en suspens de l'année précédente.

Nous nous engageons à réduire les délais de traitement et à éliminer l'arriéré de cas sur lesquels enquêter sans compromettre la qualité du travail. À cette fin, le Commissariat continue à mettre en place des mesures novatrices.

Les changements mis en œuvre ces dernières années, y compris l'embauche et la formation de nouveaux employés, ont aidé à donner un nouveau souffle à notre section chargée des enquêtes. Nous prévoyons améliorer davantage la prestation des services par les moyens suivants :

- Poursuivre les mesures d'embauche.
- Accroître l'automatisation et l'utilisation de la technologie dans le traitement des dossiers.
- Rationaliser nos processus d'enquête.

Tout ce travail est essentiel pour préserver la confiance renouvelée des Canadiennes et Canadiens envers le Commissariat et sa capacité de protéger le droit à la protection de la vie privée. Le traitement équitable, rapide et efficace des plaintes offre une occasion clé de sensibiliser le secteur privé et la population canadienne.

Plaintes déposées par la commissaire

La commissaire utilise ses pouvoirs pour déposer des plaintes sur un vaste éventail d'enjeux concernant la protection de la vie privée. Ci-dessous apparaît le sommaire de deux plaintes importantes déposées par la commissaire et résolues en 2007.

Affaire SWIFT : La circulation transfrontalière de données pose de nouveaux risques à la protection de la vie privée

En août 2006, la commissaire à la protection de la vie privée a lancé une enquête après la parution de reportages dans les journaux selon lesquels la Society for Worldwide Interbank Financial Telecommunication (SWIFT) avait communiqué au département du Trésor des États-Unis des dizaines de milliers de registres contenant des renseignements personnels.

Les documents communiqués contenaient des renseignements personnels provenant d'institutions financières canadiennes ou transférés à celles-ci. Ils incluaient vraisemblablement des données telles que les noms, adresses et numéros de compte ainsi que les sommes transférées.

Au Canada, la SWIFT recueille des renseignements personnels des banques canadiennes et lui en communique également à des fins de paiements transfrontaliers, de compensation et de règlements de valeurs mobilières et de services de trésorerie et de commerce. Sa présence au Canada est importante. La grande majorité des transferts internationaux touchant la circulation de renseignements personnels depuis et vers des institutions financières canadiennes s'effectuent au moyen du réseau de la SWIFT.

Au terme d'une enquête, la commissaire a conclu en avril 2007 que la SWIFT était assujettie à la *LPRPDÉ*, mais qu'elle ne l'avait pas enfreinte.

La commissaire a pris en note le fait que la loi permet à des organisations telles que la SWIFT de respecter les lois légitimes des autres pays où elles mènent des activités. Elle a également retenu que l'exception prévue par la *LPRPDÉ* en matière de connaissance ou de consentement s'applique à une organisation communiquant des renseignements personnels lorsqu'il y a délivrance d'une assignation à témoigner licite.

Dans l'affaire qui nous intéresse, le département du Trésor des États-Unis a commencé à délivrer des assignations à comparaître à la SWIFT en raison des données détenues dans son centre d'exploitation situé en terre américaine par suite des attaques terroristes du 11 septembre 2001.

Dans ses conclusions, la commissaire a indiqué que, si les autorités américaines avaient besoin de renseignements sur des transactions financières du côté canadien, il faudrait les inviter à utiliser les mécanismes d'information existants qui offrent un certain degré de transparence et des protections intégrées pour protéger la vie privée, comme les mécanismes canadiens de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes.

Affaire des télécommunications : Mise en lumière de l'importance de l'authentification

Le commissaire adjoint à la protection de la vie privée, Raymond D'Aoust, a déposé des plaintes contre trois compagnies canadiennes de télécommunications par suite de la publication en novembre 2005 d'un article dans le *Maclean's* décrivant la façon dont le magazine avait obtenu les relevés d'appels téléphoniques de la commissaire à la protection de la vie privée.

Les relevés avaient été achetés d'un courtier en données américain, Locatecell.com, qui les avait obtenus de Bell, TELUS Mobilité et Fido.

L'enquête a révélé que Locatecell.com avait eu recours à l'« ingénierie sociale » pour persuader des représentants du service à la clientèle des compagnies téléphoniques de

communiquer de l'information confidentielle dans les cas particuliers présumés et/ou dans des cas types ultérieurs. L'ingénierie sociale implique la manipulation des gens pour obtenir d'eux des renseignements personnels, par exemple en prétendant être une personne autorisée à obtenir l'information.

Le commissaire adjoint en a déduit que les procédures d'authentification des compagnies et la formation du personnel ne suffisaient pas à protéger adéquatement les renseignements du consommateur ou à répondre aux prescriptions de la *LPRPDÉ*.

Il a également été préoccupé par le fait que les compagnies n'en avaient pas fait suffisamment pour prévenir les employés des tactiques utilisées par les courtiers en données – même si des incidents survenus aux États-Unis avaient déjà soulevé des préoccupations.

Bien que le commissaire adjoint se soit réjoui du fait que les trois compagnies avaient revu leurs procédures d'authentification de la clientèle peu après la mise au jour des communications de renseignements, il a recommandé d'autres changements en ce qui touche la formation du personnel ainsi que les procédures relatives à l'authentification et à la communication de renseignements personnels.

Les compagnies ont mis en œuvre toutes ces mesures, sauf une, pour laquelle elles ont proposé des solutions de rechange que le commissaire adjoint a trouvées acceptables. Par conséquent, il a jugé que les plaintes étaient fondées et résolues.

Le commissaire adjoint a pris note du fait que les organisations doivent adapter leurs politiques et pratiques en matière de renseignements personnels à mesure que continuent de se poser et d'évoluer les menaces aux renseignements personnels.

Au départ, le commissaire adjoint avait également déposé une plainte contre Locatecell.com. Toutefois, les résultats préliminaires de nos demandes de renseignements ont révélé que nous n'avions pas la juridiction voulue pour poursuivre l'enquête.

Dans la foulée de ces incidents et des poursuites contre les courtiers en données aux États-Unis, les activités des courtiers ont pris fin ou ont été radicalement restreintes. Bon nombre de sites Web de courtiers ne sont pas accessibles, et celui de Locatecell.com ne fonctionne plus depuis quelque temps.

CAS PRÉSENTANT DE L'INTÉRÊT

Dans la partie suivante, on trouve un échantillon de cas sur lesquels nous avons travaillé en 2007 qui ont une importance systémique pour les enjeux liés à la protection de la vie privée au Canada.

Une décision judiciaire entraîne une enquête transfrontalière

Une décision de la Cour fédérale prise en février 2007 a annulé une décision de la commissaire à la protection de la vie privée selon laquelle elle n'avait pas la juridiction voulue en vertu de la *LPRPDÉ* pour faire enquête sur une plainte contre un courtier en données installé aux États-Unis, Accusearch Inc., et fonctionnant sous le nom d'Abika.com.

Par suite de cette décision, le Commissariat mène une enquête sur une plainte déposée par un particulier contre Accusearch. Dans le cadre de notre enquête, nous avons contacté la Federal Trade Commission des États-Unis, avec qui nous discutons activement de la manière de travailler conjointement sur des dossiers ayant trait à Accusearch.

Numéro de carte de crédit imprimé sur un billet d'avion

Un client d'une agence de voyage ayant acheté un billet d'avion a été troublé de constater qu'on avait transféré à un grossiste en voyages les renseignements figurant sur sa carte de crédit, et que le numéro complet de sa carte de crédit, y inclus la date d'expiration, était imprimé sur son billet.

La commissaire a recommandé à l'agent de voyage de mieux informer ses clients du fait que leurs renseignements personnels seraient transférés aux grossistes.

En outre, elle a recommandé à l'agence de confirmer les pratiques du grossiste en matière de manipulation des renseignements, car elle avait constaté que le grossiste hésitait à révéler ses pratiques – bien qu'il existait un contrat afférent entre les deux parties.

L'agence a plus tard informé le Commissariat qu'elle ne ferait plus affaire avec le grossiste.

Jusqu'à ce que cesse complètement la production de billets en papier (en décembre 2007), la commissaire a recommandé à l'agence d'expliquer aux clients que les renseignements sur la carte de crédit apparaîtraient sur les billets en papier. En outre, l'agence doit leur offrir l'option d'un billet électronique, qui ne contient pas ces renseignements.

Un agent d'assurance communique de l'information sans consentement approprié

Une personne s'est plainte du fait qu'un administrateur de prestations d'assurance médicale avait communiqué de manière inappropriée des renseignements personnels délicats à son employeur, en dépit du fait qu'elle avait signé un formulaire de consentement limité en matière de communication de renseignements.

Au moment de faire une demande de prestations d'invalidité de longue durée, la personne en cause a négocié une entente de consentement à diffusion restreinte avec l'évaluateur de la compagnie d'assurance dans le but exprès de restreindre le droit de l'assureur de transférer les renseignements médicaux à son employeur.

Des mois plus tard, une agente en réadaptation pour le compte de compagnies d'assurance, dont l'employeur du plaignant avait retenu les services, croyait avoir le consentement verbal du plaignant pour informer son employeur qu'il était prêt à retourner au travail.

Elle a donc expédié par courriel à l'employeur des extraits du rapport d'un spécialiste médical – même si le plaignant lui avait rappelé les instructions du consentement limité.

La commissaire à la protection de la vie privée en a déduit que la communication de renseignements n'était pas appropriée et qu'il aurait fallu obtenir le consentement écrit. La commissaire a recommandé à la compagnie de mettre à jour ses politiques et sa formation. La compagnie a suivi ces recommandations.

Une compagnie de télécommunications néglige d'obtenir le consentement l'autorisant à enregistrer les appels

Une personne s'est plainte du fait qu'une compagnie de télécommunications n'obtenait pas le consentement approprié avant d'enregistrer ses appels sortants.

La compagnie avait téléphoné à la mère du plaignant, mais ne l'avait pas informée qu'elle enregistrait l'appel. La politique de la compagnie exige des employés qu'ils informent les gens de l'enregistrement des appels entrants, mais non sortants.

Selon la compagnie, une déclaration dans sa politique écrite sur la protection de la vie privée était un moyen suffisant d'obtenir le consentement l'autorisant à enregistrer les appels sortants, ce avec quoi n'était pas d'accord la commissaire à la protection de la vie privée.

Elle a recommandé à la compagnie d'informer les clients dès le début de chaque appel de marketing sortant que la conversation serait enregistrée ou surveillée d'une autre manière et de leur expliquer pourquoi elle agit ainsi.

La compagnie de télécommunications a accepté de mettre en œuvre les recommandations.

Une station de télévision agit de manière à enregistrer secrètement les appels d'une employée

Un syndicat représentant les employés d'une station de télévision dans une petite communauté a allégué qu'un gestionnaire avait installé de l'équipement d'enregistrement des appels téléphoniques dans le poste de travail d'une représentante du service à la clientèle. La station aurait enregistré sur ruban ses conversations téléphoniques sans sa connaissance et son consentement.

L'enquête a confirmé la véracité de l'allégation. Nous avons extrait d'un dossier dans l'ordinateur de la plaignante une conversation enregistrée entre elle et son conjoint. La plaignante nous a dit qu'elle ne savait pas que l'appel était enregistré.

Interrogé, l'employeur a soutenu que l'équipement n'était pas encore opérationnel et qu'on l'avait installé pour faire un essai, dans l'intention d'enregistrer des conversations au cas où surviendrait un désaccord de facturation ainsi que pour dissuader les clients injurieux.

Puisque la station avait l'intention d'installer un tel équipement dans tous les postes de travail des représentants du service à la clientèle, la commissaire adjointe lui a recommandé d'informer à l'avance les employés de ses plans et de l'objectif poursuivi. Elle lui a également indiqué qu'elle devait informer ses clients que leurs appels pouvaient être enregistrés et leur expliquer la raison d'une telle démarche.

On a considéré que la plainte était fondée et résolue. La station a décidé en bout de ligne de ne pas enregistrer les appels.

Les règles d'un concours comportaient un avertissement adéquat selon lequel il y aurait partage des adresses de courriel

Un abonné du bulletin d'une entreprise s'est inscrit à son concours afin de gagner des vacances pour quatre personnes. Il a fourni les adresses de courriel d'autres personnes de manière à avoir plusieurs inscriptions au concours.

Toutefois, il a été consterné en voyant que les courriels expédiés par la compagnie à ces autres personnes étaient conçus de manière à donner l'impression qu'ils provenaient de lui-même. Plus particulièrement, il était renversé de voir que son ex-épouse avait reçu un courriel dans lequel il donnait censément à entendre que les deux voyageraient ensemble s'il gagnait le concours.

Il s'est plaint du fait qu'on s'était servi de son nom dans les courriels sans son consentement.

La commissaire adjointe à la protection de la vie privée a conclu que la plainte n'était pas fondée. Les règles du concours et leur formulation indiquaient clairement que les messages par courriel aux personnes en référence seraient personnalisés comme si le concurrent les avait lui-même expédiés. Étant donné que le prix consistait en un voyage pour quatre personnes, elle a estimé raisonnable de s'attendre à ce que le message suggère que l'abonné et le destinataire du courriel voyageraient ensemble.

Enquêtes sur des incidents

Le Commissariat mène également des enquêtes sur des incidents ayant trait à des violations possibles de la *LPRPDÉ*. Nous recevons des rapports de déclaration volontaire d'incidents de la part d'organisations, des rapports des médias sur des atteintes possibles à la sécurité des données, et de l'information de gens qui aimeraient que nous nous penchions sur un dossier, mais qui ne sont pas nécessairement touchés par l'affaire.

Entre autres exemples d'incidents du genre, mentionnons des reçus de carte de crédit trouvés dans des bennes à rebuts ou des rapports d'atteintes à la sécurité de l'information sur les sites Web.

Lorsqu'on porte un incident à notre attention, nous travaillons avec l'organisation responsable à corriger toute lacune et résolvons les affaires restantes telles que l'envoi d'avis aux clients touchés, l'extraction de l'information, et l'assurance que sont mises en œuvre des mesures de sécurité appropriées.

En 2007, nous avons mené 12 enquêtes sur des incidents portés à notre attention d'une source autre que l'organisation directement impliquée dans l'incident.

Déclaration volontaire d'atteintes à la sécurité des données

Malgré le fait que les lois relatives à la protection des renseignements personnels existent depuis plusieurs années, ce ne sont pas toutes les organisations qui disposent de politiques et procédures claires concernant les atteintes à la sécurité des données. Cela dit, nous estimons que les gens sont davantage sensibilisés à la nécessité d'avertir le Commissariat des atteintes à la sécurité des données et aussi d'informer les clients

touchés – ce qui découle en partie de l'élaboration et de la publication de nos lignes directrices sur les atteintes à la sécurité des données.

Les organisations ont volontairement déclaré 34 atteintes en 2007, par rapport à 20 l'année précédente. Les atteintes à la sécurité des données signalées par l'intéressé en 2007 ont compromis les renseignements personnels de quelque 50 000 personnes.

Bien que différents secteurs commencent à nous signaler des atteintes à la sécurité des données, notamment des groupes de recherche et des compagnies publicitaires, l'essentiel de ces avis continue de provenir des industries du domaine bancaire, des télécommunications et du commerce de détail.

Il vaut la peine de mentionner que la moitié des atteintes qui nous ont été rapportées avaient trait à des données électroniquement stockées – c'était souvent le fait de renseignements sur les consommateurs stockés dans des ordinateurs portatifs volés. De plus, nous avons découvert que près de neuf personnes sur dix touchées par une atteinte déclarée par l'intéressé se trouvaient en situation de risque étant donné que leurs renseignements personnels étaient détenus sur support électronique non sécurisé ou non doté de mécanismes de protection comme des coupe-feu et des procédés de cryptage.

Nous nous réjouissons de constater que les organisations nous faisant des déclarations volontaires agissent en temps opportun – souvent moins d'un jour ou deux suivant l'incident. Un avis rapide nous aide à nous préparer aux demandes de renseignements des médias ou aux plaintes qui suivent l'avis expédié aux personnes touchées. La déclaration volontaire nous permet également de recueillir des statistiques et de sensibiliser les organisations et le public sur les causes des atteintes à la sécurité des données ainsi que sur les mesures préventives recommandées.

Voici de brèves descriptions de certaines atteintes rapportées au Commissariat en 2007 :

- L'employé d'une firme sous contrat avec une institution financière s'est fait voler son ordinateur portatif à son domicile. L'ordinateur contenait les renseignements personnels de plusieurs centaines d'employés, sauf que ces renseignements n'étaient pas considérés comme délicats. L'institution financière et la firme sous contrat avaient en place des contrôles pertinents pour protéger les renseignements personnels, mais l'employé ne les a pas appliqués. Par suite de cet incident, l'établissement a mis en place des contrôles additionnels tels que des logiciels de chiffrement.

- Un voleur s'est emparé d'un ordinateur portatif dans le véhicule d'un employé d'une société de services financiers. Cet ordinateur contenait des registres de la clientèle. Plus de la moitié de ces registres révélaient des numéros d'assurance

sociale et de compte. L'entreprise a avisé les personnes concernées et instauré des alertes sur les comptes des clients touchés.

- Il y a eu vol de l'ordinateur portatif d'un employé d'une agence faisant la promotion d'un événement dans un casino. L'ordinateur portatif, qui était dans une voiture lors du vol, contenait une base de données protégée par un mot de passe et contenant de l'information sur certains des participants à l'événement, sauf que les données n'étaient pas cryptées. Les renseignements personnels incluaient le nom et l'âge des participants, leurs coordonnées, les numéros de leurs permis de conduire et, dans un cas, les numéros du passeport et de la carte Santé. Par suite de l'incident, l'agence a informé les personnes touchées et leur a offert des arrangements pour la surveillance du crédit. Elle a également adopté plusieurs mesures de sécurité, comme des logiciels cryptographiques sur les ordinateurs portatifs, et a rappelé aux employés les politiques et procédures de sécurité. L'employé responsable de la perte des données a été congédié.

Nous espérons que la sensibilisation croissante des gens à la nécessité d'informer le Commissariat et les personnes touchées lorsqu'il se produit une atteinte à la vie privée se traduira sous peu en mesures de sécurité plus efficaces. Nous continuons à exhorter les particuliers comme les organisations à prendre des précautions de base pour sécuriser les données, par exemple :

- Limiter la quantité de renseignements personnels recueillis, utilisés et transportés par le truchement de dispositifs électroniques.

- Ne jamais laisser sans surveillance un ordinateur portatif dans des situations où on pourrait le dérober.

- Utiliser des technologies qui rehaussent le niveau de sécurité et de protection de la vie privée telles que les services de chiffrement des données et de préservation de l'anonymat.

- Utiliser des mots de passe difficiles à trouver.

- Éviter le recours aux caractéristiques d'accès automatique qui sauvegardent les noms et mots de passe.

- S'assurer que les renseignements personnels dans un disque dur sont entièrement écrasés – pas seulement effacés – avant de jeter au rebut ou de vendre un ordinateur.

En suivant ces étapes, les organisations peuvent considérablement réduire le risque de compromission des renseignements personnels qu'elles détiennent.

VÉRIFICATION ET REVUE

Les vérifications représentent l'un des outils de conformité prévus par la *LPRPDÉ*. La commissaire à la protection de la vie privée a le pouvoir de vérifier les pratiques d'une organisation en ce qui touche la gestion des renseignements personnels dans les cas où elle a des motifs raisonnables de croire que ces pratiques ne sont pas conformes à la Loi.

Lorsqu'une vérification est amorcée en vertu de la *LPRPDÉ*, le vérificateur dispose du pouvoir délégué de recevoir des preuves des témoins, de pénétrer dans un local à toute heure raisonnable, et d'examiner des registres trouvés sur les lieux ou d'obtenir des copies de tels registres. Au besoin, la commissaire à la protection de la vie privée peut obliger des gens à fournir des preuves.

Au terme d'une vérification, nous fournissons à l'organisation un rapport de nos conclusions et toute recommandation que la commissaire estime appropriée. Le rapport peut être divulgué s'il en va de l'intérêt du public.

Le Commissariat réalise également des vérifications auprès des institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels*.

Le but des vérifications – dans le secteur privé comme dans le secteur public – consiste à promouvoir la responsabilisation et la conformité aux lois, politiques et normes applicables, et aussi à contribuer à l'amélioration des systèmes et pratiques de protection de la vie privée.

Cadre pour amorcer des vérifications en vertu de la *LPRPDÉ*

L'une des questions les plus fréquemment posées par les organisations assujetties à la *LPRPDÉ* pourrait être : Sur quoi vous fondez-vous pour mener ou non une vérification?

La décision de mener ou non une vérification est prise en fonction de chaque cas. La loi exige de la commissaire d'avoir des motifs raisonnables de croire qu'il y a non-conformité à la Loi pour mener une vérification.

En 2007, nous avons élaboré un cadre pour amorcer des vérifications qui donne un certain aperçu du processus de sélection des vérifications.

Comment décidons-nous s'il y a lieu de faire une vérification en vertu de la *LPRPDÉ*?

Plans stratégiques

Le Plan stratégique et le Rapport annuel sur les plans et les priorités du Commissariat décrivent les résultats que nous voulons obtenir. Tout au long du processus visant à déterminer s'il y a lieu de mener une vérification, nous prenons en considération le mandat, les objectifs, les plans et les priorités du Commissariat.

Analyse des enjeux

PRINCIPE 1 : Existe-t-il des facteurs, ou s'est-il produit des incidents, qui indiquent un risque de non-conformité à la Loi ou l'absence de saines pratiques de gestion de la protection des renseignements personnels?

Ce processus comprend la détermination, l'analyse et la confirmation des enjeux relatifs à la protection des renseignements personnels d'une industrie, d'une entité ou d'un programme, et si possible, un examen préliminaire des principales fonctions de contrôle de la gestion des renseignements personnels. L'analyse des enjeux est généralement menée à l'interne et basée sur de l'information recueillie par le CPVP au moyen d'enquêtes et de recherches, mais elle peut comporter plusieurs interventions, y compris des enquêtes auprès de la direction. Voici certains des facteurs qui peuvent indiquer l'absence de saines pratiques de gestion des renseignements personnels : rapports crédibles des médias, recommandations de comités parlementaires, contraventions révélées par des dénonciations, enquêtes sur un incident, résultats d'enquêtes sur des plaintes, demande d'examen d'une entité ou de l'industrie, résultats d'études empiriques ou sondages dans l'industrie.

Motifs

PRINCIPE 2 : Existe-t-il des preuves suffisantes et crédibles indiquant une forte possibilité qu'une vérification révèle une contravention à la Loi?

Ce qui constitue un motif raisonnable repose sur l'examen de l'information recueillie durant les activités d'analyse des enjeux et sur le processus visant à décider s'il existe des motifs suffisants pour justifier que le Commissariat exerce son pouvoir discrétionnaire en vertu du paragraphe 18(1) de la Loi. À l'interne, le CPVP établit des fondements clairs pour la vérification et s'assure que le seuil de preuve est adéquat.

Action

PRINCIPE 3 : Compte tenu des résultats de l'analyse des enjeux et du processus d'établissement des motifs raisonnables, quelles mesures permettraient le mieux de promouvoir et d'encourager la conformité et l'application de saines pratiques de gestion des renseignements personnels? La vérification est-elle la meilleure approche et le secteur examiné se prête-t-il bien à une vérification?

Le Commissariat reconnaît qu'aucun outil ou instrument ne suffit à lui seul à faire respecter la conformité dans toutes les situations. C'est pourquoi il examine tous les moyens à sa disposition, y compris la vérification, pour encourager la conformité et promouvoir de saines pratiques de gestion des renseignements personnels. La décision finale de procéder à une vérification dépend de nombreuses considérations comme la nature de l'affaire, l'importance des risques systémiques, la fréquence à laquelle le problème a été observé, l'ampleur des mesures correctives prises, les résultats et les conclusions des enquêtes terminées et en cours sur la protection des renseignements personnels et les positions antérieures du Commissariat.

Dossier indiquant les critères sur lesquels se base le Commissariat pour décider de procéder à une vérification.

Vérifications d'Equifax et de TransUnion

La commissaire à la protection de la vie privée a complété des vérifications simultanées des systèmes d'identification et d'authentification en ligne des agences d'évaluation du crédit Equifax Canada et TransUnion.

La société Equifax a entrepris une poursuite dans le cadre de laquelle elle remettait en question l'existence de motifs raisonnables justifiant la décision de la commissaire à la protection de la vie privée de procéder à une vérification. Bien qu'Equifax ait maintenu tout au long du processus que la vérification ne reposait pas sur des motifs raisonnables, la vérification a été conclue. Un rapport a été remis à Equifax, et aucune autre mesure n'était requise de la part d'Equifax par suite de cette vérification.

TransUnion estimait également que la commissaire n'avait pas de motifs raisonnables, mais a choisi de ne pas intenter de poursuite. Comme ce fut le cas avec la vérification d'Equifax, TransUnion a reçu un rapport et aucune autre mesure n'était requise de sa part par suite de cette vérification.

Outil d'auto-évaluation

Le Commissariat prépare un outil pour aider les organisations à évaluer leur conformité à la *LPRPDÉ* et à ses principes relatifs à l'équité dans le traitement des renseignements. Cet outil aidera les organisations à diagnostiquer les problèmes posés par leurs systèmes et pratiques de protection de la vie privée.

Nous sollicitons des observations sur ce nouvel outil d'auto-évaluation de plusieurs responsables de la protection des renseignements personnels des grandes entreprises, de professeurs d'université, de chefs de file en formation et perfectionnement des gestionnaires ainsi que d'associations de gens d'affaires et d'associations professionnelles.

Nous nous attendons à disposer en 2008 d'une version finale pour les moyennes et grandes entreprises.

DEVANT LES TRIBUNAUX

La commissaire à la protection de la vie privée peut intenter des poursuites lorsqu'une organisation refuse d'adopter ses recommandations dans des cas fondés, ce qui a aidé à établir un niveau élevé de conformité aux recommandations.

En vertu de l'article 14 de la *LPRPDÉ*, un plaignant ou la commissaire à la protection de la vie privée peut, dans certaines circonstances, demander une audience à la Cour fédérale pour toute question évoquée dans le rapport de la commissaire.

L'article 15 permet également à la commissaire à la protection de la vie privée, avec le consentement du plaignant, de demander directement une audience à la Cour fédérale concernant une affaire visée par l'article 14. Conformément à cet article, la commissaire peut comparaître devant la Cour fédérale au nom de tout plaignant ayant demandé une audience en vertu de l'article 14. Elle peut également, avec la permission de la Cour fédérale, comparaître comme partie à toute audience en vertu de l'article 14 non demandée par elle-même.

Depuis notre compte rendu de la situation des procédures en cours dans notre rapport annuel de 2006 sur la *LPRPDÉ*, de nouvelles demandes ont été produites, et certains litiges ont été résolus. Nous discutons ci-dessous de ces nouveaux développements.

Conformément à la lettre et à l'esprit de notre mandat, nous avons respecté la vie privée des plaignants en retirant leur nom.

Causes réglées

En 2007, plusieurs demandes de nature judiciaire déposées contre des organisations ont été réglées avant que la Cour fédérale ne les ait entendues et qu'elle n' ait rendu une décision.

X. c. ING Canada Inc.
N° de dossier de la Cour fédérale : T-1283-07

Un plaignant a fait une demande de contrôle judiciaire en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*. Le CPVP a amorcé un processus de médiation, et par suite d'une entente négociée, le plaignant a retiré sa demande.

X. c. Brampton Flying Club
N° de dossier de la Cour fédérale : T-192-05

Un plaignant a demandé une audience en vertu de l'article 14 parce qu'il alléguait que Brampton Flying Club avait négligé de lui donner accès à ses renseignements personnels dans les 30 jours suivant sa demande écrite et qu'on avait tenté de lui imposer un montant déraisonnable pour répondre à sa demande. Cette affaire a été réglée par les parties en janvier 2007.

X. c. Laidlaw Transit Ltd.
N° de dossier de la Cour fédérale : T-684-07

Un plaignant a demandé une audience en vertu de l'article 14 pour contester une forme de surveillance en milieu de travail entreprise par Laidlaw Transit Ltd. Le CPVP a servi de médiateur dans le différend. Le plaignant a renoncé à sa demande, et les parties sont parvenues à une entente.

X. c. La Banque de Nouvelle-Écosse
N° de dossier de la Cour fédérale : T-2126-05

Cette affaire concernait une plainte selon laquelle un ou plusieurs employés de la Banque de Nouvelle-Écosse avaient obtenu des renseignements personnels sans consentement et communiqué ces renseignements à un tiers. Le plaignant a renoncé à sa demande d'audience devant la Cour fédérale, et l'affaire a été réglée entre les parties.

Commissaire à la protection de la vie privée du Canada c. Air Canada
N° de dossier de la Cour fédérale : T-342-07

La commissaire à la protection de la vie privée a demandé une audience à la Cour fédérale afin d'amener Air Canada à mettre en œuvre ses recommandations dans une affaire portant sur l'ampleur des renseignements médicaux personnels recueillis par l'organisation lorsqu'elle voulait s'assurer de la capacité d'un employé de retourner au travail.

Les parties ont réglé le différend. Air Canada a mis en œuvre les recommandations de la commissaire à notre satisfaction.

Litiges en cours

Les litiges en cours ont trait à des demandes de contrôle judiciaire en vertu de l'article 18.1 de la *Loi sur les Cours fédérales* et à des demandes d'audience déposées par des plaignants en vertu de l'article 14 de la *LPRPDÉ* dans laquelle le CPVP était impliqué comme partie ou comme intervenant.

Dans une affaire digne de mention, la State Farm Mutual Automobile Insurance Company a remis en question le pouvoir de la commissaire à la protection de la vie privée de faire enquête sur un refus de donner accès à des renseignements personnels et d'exiger la production de documents durant le déroulement de l'enquête.

En juillet 2007, State Farm a demandé une audience à la Cour du Banc de la Reine du Nouveau-Brunswick pour faire une déclaration selon laquelle :

- La *LPRPDÉ* ne s'appliquait pas à la communication de renseignements personnels réclamés par un plaignant.
- La *LPRPDÉ* a été édictée hors des pouvoirs attribués au Parlement fédéral.
- La commissaire à la protection de la vie privée n'avait pas le pouvoir de faire enquête sur la plainte en question.
- La commissaire à la protection de la vie privée n'avait pas le pouvoir d'exiger la production des renseignements demandés.

La commissaire à la protection de la vie privée a présenté une motion préliminaire pour que la demande de State Farm soit refusée ou mise en sursis en raison du fait que la Cour fédérale était le forum le plus indiqué.

La motion a été accueillie en janvier 2008 d'après le motif que la Cour fédérale était le forum le plus indiqué pour évaluer la demande, qui impliquait des questions de validité constitutionnelle et le contrôle judiciaire du pouvoir de la commissaire à la protection de la vie privée. L'appel de cette décision interjeté par State Farm sera entendu au début de 2008. De plus amples renseignements seront fournis dans notre prochain rapport annuel.

D'autres décisions judiciaires importantes rendues en 2007 apparaissent ci-dessous.

***Demandes de contrôle judiciaire en vertu de l'article 18.1 de la* Loi sur les Cours fédérales**
Blood Tribe Department of Health c. commissaire à la protection de la vie privée du Canada et autres
N° de dossier de la Cour suprême du Canada : 31755

Nous avons relaté les détails de cette affaire en cours dans nos trois derniers rapports annuels. En jeu se trouvent le secret professionnel qui lie un avocat à son client et notre capacité d'obtenir les renseignements dont nous avons besoin pour mener nos enquêtes. Le résultat final – qui reste à venir – aura des répercussions profondes sur la manière dont nous menons nos enquêtes.

L'affaire a débuté lorsqu'une femme ayant perdu son emploi au sein du Blood Tribe Department of Health a demandé son dossier personnel d'emploi, ce qu'on lui a refusé.

Cette femme a porté plainte au Commissariat. Dans le cadre de notre enquête, nous avons demandé une copie du dossier personnel de la plaignante. Le Blood Tribe Department of Health a fourni certains registres, mais a fait valoir que les autres documents étaient protégés par le secret professionnel et a refusé de les remettre.

Nous étions d'avis qu'il nous fallait ces documents pour vérifier en toute indépendance si l'on pouvait soustraire à la communication les renseignements personnels demandés par une plaignante sous prétexte que ces renseignements sont protégés par le secret professionnel.

Nous avons rendu une ordonnance pour que l'organisation produise les documents. Le Blood Tribe Department of Health est allé devant le tribunal pour contester le pouvoir de la commissaire à la protection de la vie privée de rendre une telle ordonnance – ce qui a interrompu l'enquête.

La Cour fédérale a rejeté la demande de contrôle judiciaire du Blood Tribe Department of Health.

Toutefois, la Cour d'appel fédérale a annulé l'ordonnance de la commissaire à la protection de la vie privée, en s'appuyant sur le fait que le libellé de la *LPRPDÉ* n'est pas suffisamment clair pour accorder à la commissaire le pouvoir particulier d'ordonner la production de documents protégés par le secret professionnel. La Cour nous a proposé de procéder en fonction de chaque cas lorsque nous voulons obtenir de la part de la Cour fédérale le droit d'examiner des documents protégés par le secret professionnel dans le contexte des plaintes impliquant un accès refusé à des renseignements personnels.

Nous avons porté cette décision en appel devant la Cour suprême du Canada, qui a prévu une audience le 21 février 2008.

La commissaire à la protection de la vie privée a indiqué qu'elle prévoit revoir la question avec le ministre de l'Industrie dans le cas où il faudrait modifier la *LPRPDÉ* par suite d'une décision de la Cour suprême.

X. c. Accusearch Inc., s/n Abika.com et autres
N° de dossier de la Cour fédérale : T–2228–05

Une personne a fait une demande de contrôle judiciaire pour obtenir une ordonnance d'annulation ou de cassation de la décision de la commissaire adjointe à la protection de la vie privée, qui affirmait ne pas disposer du pouvoir de faire enquête sur une plainte contre Accusearch Inc., une organisation américaine faisant affaire sous le nom d'Abika.com.

Note : Nous avons également relaté cette affaire dans notre rapport annuel de 2006.

La personne souhaitait qu'on examine la position de la commissaire adjointe selon laquelle elle estimait ne pas avoir la compétence voulue pour faire enquête. En février 2007, la Cour fédérale a accueilli la demande en s'appuyant sur le fait que la commissaire adjointe avait la compétence voulue pour faire enquête sur la circulation transfrontalière des renseignements personnels dans un tel cas.

Il s'agit d'une décision importante pour le Commissariat en ce qu'elle a aidé à renforcer nos activités d'engagement internationales afin de mieux protéger les renseignements personnels des Canadiennes et Canadiens.

Par suite de cette décision, nous enquêtons sur la plainte contre Accusearch.

De plus, des poursuites ont été intentées aux États-Unis contre Accusearch en ce qui a trait à la publicité et à la vente de dossiers d'appels téléphoniques confidentiels à des tiers sans le consentement des personnes concernées. Étant donné l'intérêt grandissant du Commissariat pour les activités internationales aidant à protéger les renseignements personnels des Canadiennes et Canadiens, nous surveillons ces poursuites de près.

***Demandes au tribunal déposées par le plaignant en vertu de l'article 14 de la* LPRPDÉ**
Dr Jeffrey Wyndowe (Psychiatric Assessment Services Inc.) c. X.
N° de dossier de la Cour d'appel fédérale : A–551–06

Il s'agit d'une affaire qui dure depuis longtemps, et dont nous avons discuté dans nos rapports annuels de 2005 et 2006. La question en jeu est de savoir si une personne a le droit d'accéder à ses renseignements personnels contenus dans des notes prises par un médecin lorsqu'il effectue un examen médical indépendant au nom d'une compagnie d'assurance.

La Cour fédérale a examiné la question de savoir si de telles notes contenaient les renseignements personnels de la personne ayant été examinée, et le cas échéant, s'il s'appliquait des exceptions aux termes de la *LPRPDÉ* permettant de refuser l'accès à de tels renseignements. Selon la Cour fédérale, les notes contenaient effectivement les renseignements personnels de la personne concernée, et les prétentions d'exception en vertu de la *LPRPDÉ* ne s'appliquaient pas. Par conséquent, elle a ordonné au médecin de donner accès aux notes.

Le médecin a interjeté appel de la décision. Devant la Cour d'appel fédérale, les questions en jeu étaient de savoir, premièrement, si les notes constituaient les renseignements personnels de la personne examinée ou le produit du travail du médecin; et deuxièmement, si les notes prises dans le contexte d'un examen médical indépendant surviennent dans le cours d'une activité commerciale visée par la *LPRPDÉ*.

La Cour d'appel fédérale a rendu sa décision en février 2008. On y lisait que :

(i) Les notes prises par un médecin examinateur dans le cadre d'un examen médical indépendant à la demande d'une compagnie d'assurance sont consignées au « cours d'une activité commerciale », de sorte qu'elles sont clairement visées par la *LPRPDÉ*.

(ii) Les notes prises par un médecin examinateur dans le cadre d'un examen médical indépendant contiennent clairement des renseignements sur la santé d'une personne, et par voie de conséquence, des renseignements personnels.

La Cour d'appel fédérale a soutenu que la personne avait le droit d'accéder aux parties des notes qui contenaient des renseignements fournis par elle, et de corriger toute erreur que l'examinateur médical pourrait avoir faite.

Toutefois, le tribunal en a également déduit que les renseignements dans les notes pouvaient être personnels à la fois pour la personne et le médecin, et qu'il pourrait être nécessaire de parvenir à un équilibre en prenant en considération les intérêts privés de la personne et ceux du médecin, ainsi que l'intérêt public associé à la communication et à la non-communication.

On a retourné l'affaire à la commissaire à la protection de la vie privée de manière à ce qu'elle puisse, de concert avec l'avocat du médecin, déterminer les parties des notes qui contiennent les renseignements personnels de la personne et qu'il faudrait communiquer.

X. c. Telus Communications Inc.
N° de dossier de la Cour d'appel fédérale : A–639–05

Cette affaire impliquait des plaintes d'employés de Telus sur la mise en œuvre par la compagnie d'un système de reconnaissance vocale.

Note : Nous avons également relaté cette affaire dans nos rapports annuels de 2004, 2005 et 2006.

En janvier 2007, la Cour d'appel fédérale confirmait que :

(i) L'empreinte vocale recueillie par Telus constitue des renseignements personnels.

(ii) Dans les faits, une personne raisonnable trouverait raisonnable dans les circonstances qu'une entreprise adopte une technologie d'empreinte vocale à des fins d'authentification et de sécurité.

(iii) Ce système d'authentification par empreinte vocale de Telus répond aux prescriptions de la *LPRPDÉ* en matière de consentement puisque les employés ne pouvaient être inscrits dans le système sans leur consentement actif.

(iv) Aucune des exceptions énoncées dans l'article 7 de la *LPRPDÉ* prévoyant la collecte sans consentement ne s'applique à la situation.

(v) Telus a adéquatement informé ses employés des conséquences éventuelles s'ils refusaient d'accorder leur consentement.

X. c. Scotia Capital Inc.
N° de dossier de la Cour fédérale : T-2181-05

En réponse à une demande d'un plaignant souhaitant accéder à ses renseignements personnels, Scotia Capital a remis au plaignant une copie de ses renseignements personnels, excluant toutefois ses talons de chèque de paye ou les registres de ses heures de travail.

Le plaignant prétendait que Scotia Capital invoquait de manière inappropriée des exceptions liées à de l'information provenant d'un tiers et à des documents protégés par secret professionnel. Par suite de notre enquête, l'entreprise a expédié des renseignements additionnels au plaignant.

La commissaire adjointe a conclu que l'organisation avait par ailleurs raison de retenir des renseignements qui contenaient des renseignements personnels d'autres personnes ou étaient protégés par le secret professionnel.

Le plaignant a fait une demande d'audience auprès de la Cour fédérale en vertu de l'article 14 de la *LPRPDÉ*. La demande a été rejetée par la suite.

X. c. J.J. Barnicke Ltd.
N° de dossier de la Cour fédérale : T-1349-06

Une personne a porté plainte contre J.J. Barnicke Ltd. en prétendant que la société recueillait des renseignements personnels de façon inappropriée et appliquait des politiques inadéquates pour les protéger. Le vice-président de la compagnie avait expédié un courriel à tous les employés demandant si quelqu'un connaissait l'entreprise pour laquelle travaillait le plaignant.

Selon la commissaire adjointe à la protection de la vie privée, comme il n'y avait aucune preuve qu'un employé de J.J. Barnicke avait répondu au courriel, il n'existait aucune collecte de renseignements personnels comme tel. Par conséquent, la plainte concernant la collecte abusive de renseignements personnels n'était pas fondée.

Toutefois, l'enquête a révélé que J.J. Barnicke n'avait pas en place de politiques ou procédures adéquates en matière de protection de la vie privée, ni ne comptait sur un agent désigné de la protection de la vie privée responsable de la conformité. Bien que J.J. Barnicke ait élaboré une telle politique durant l'enquête, la commissaire adjointe à la protection de la vie privée a recommandé que l'organisation affiche cette politique sur son site Web, distribue cette politique à ses employés et donne au personnel une formation adéquate concernant la protection de la vie privée. J.J. Barnicke a pleinement mis en œuvre les recommandations de la commissaire adjointe.

Le plaignant s'est adressé à la Cour fédérale. Il y eu ajournement d'une audience prévue pour novembre 2007 en raison d'une motion de procédure préliminaire, sans toutefois qu'une nouvelle date d'audience n'ait été fixée.

Fonction de surveillance

Dans le cadre de notre rôle de surveillance des décisions judiciaires au sens large, le Commissariat à la protection de la vie privée continue de surveiller certaines affaires judiciaires impliquant de nouvelles questions d'actualité au chapitre de la protection de la vie privée. C'est l'une des façons par lesquelles nous demeurons au fait des progrès de droit réalisés, que ce soit au moyen de demandes en vertu de la *LPRPDÉ*, de la *Loi sur*

la protection des renseignements personnels, de la *Loi sur l'accès à l'information* à l'échelon fédéral ou même de poursuites entendues par des tribunaux provinciaux de haute instance au titre de la common law ou du droit civil du Québec.

À titre d'exemple, on nous a accordé le statut d'intervenant dans l'affaire *X. c. le ministre de la Santé et la commissaire à la protection de la vie privée du Canada*, même si l'affaire découlait d'abord de la *Loi sur l'accès à l'information*.

Dans cette affaire, un journaliste cherchait à accéder à la base de données du système canadien d'information sur les effets indésirables des médicaments de Santé Canada, qui contient des déclarations obligatoires et volontaires sur les effets indésirables des médicaments mis en vente au Canada.

Santé Canada a refusé de révéler la province dans laquelle les données avaient été recueillies en invoquant le fait que cette information, en plus de l'information déjà diffusée, pourrait permettre d'identifier des personnes si on les combinait à des renseignements publiquement accessibles. Le commissaire à l'information était d'accord, faisant valoir que les renseignements étaient soustraits à l'application de la loi sur l'accès.

Le journaliste a demandé à ce que la décision de Santé Canada fasse l'objet d'un contrôle judiciaire.

Le Commissariat a décidé d'intervenir compte tenu de l'importance de l'affaire pour l'interprétation et l'application de la *LPRPDÉ* et de la *Loi sur la protection des renseignements personnels*, ainsi que pour l'interprétation du sens de l'expression « renseignements personnels ». Nous avons plaidé en faveur d'une définition étendue.

Cette affaire démontre le rôle important que nous pouvons jouer comme intervenant sur des questions ayant de profondes répercussions sur la *LPRPDÉ* et/ou sur la *Loi sur la protection des renseignements personnels* – contribuant ainsi de façon valable à l'évolution de la jurisprudence en matière de protection de la vie privée au Canada.

La Cour fédérale devait entendre l'affaire en février 2008.

LOIS PROVINCIALES ET TERRITORIALES ESSENTIELLEMENT SIMILAIRES

Selon le paragraphe 25(1) de la *LPRPDÉ*, le Commissariat est tenu de déposer annuellement devant le Parlement un rapport sur « la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la Loi.

Dans les rapports annuels passés, nous avons fait rapport sur la législation en Colombie-Britannique, en Alberta, en Ontario et au Québec, qui a été déclarée essentiellement similaire.

Aucune province ni aucun territoire n'a adopté en 2007 de loi pour laquelle on a demandé le statut de loi essentiellement similaire à la *LPRPDÉ*.

L'ANNÉE QUI VIENT

Nos priorités clés pour l'année à venir sont les suivantes :

Continuer à améliorer la prestation des services

- Concevoir et mettre en œuvre des stratégies d'enquête nouvelles et novatrices pour améliorer l'efficacité de notre processus de résolution des plaintes.

Développer des capacités organisationnelles durables

- Sur le plan des ressources humaines, se pencher sur la question du maintien en place de l'effectif et élargir le Commissariat afin d'équilibrer la charge de travail à l'interne et de gérer la demande croissante pour ce qui est de nos services.
- Poursuivre un projet de renouvellement de la gestion de l'information; adopter la technologie du balayage; utiliser les technologies actuelles pour mettre à jour les processus d'enquête et de demandes de renseignements; moderniser notre système de gestion des cas.

Aider les Canadiennes et Canadiens à prendre des décisions éclairées en matière de protection de la vie privée

- Élaborer du matériel pour aider les Canadiennes et Canadiens à mieux comprendre leur droit à la protection de la vie privée et à prendre des mesures pour protéger ce droit.
- Préparer et distribuer des publications et des lignes directrices sur supports imprimé et électronique; continuer d'entrer en contact avec les gens au moyen de technologies nouvelles et interactives telles que des blogues et des vidéos en ligne.
- Mettre en œuvre une campagne de marketing social sur la protection de la vie privée des enfants en ligne.
- Mettre en place des programmes de sensibilisation et d'éducation en partenariat avec les commissaires à la protection de la vie privée des provinces et des territoires.

Exercer du leadership pour promouvoir quatre questions prioritaires en matière de protection de la vie privée

- Technologie de l'information

- Développer suffisamment de capacités pour évaluer les répercussions des nouvelles technologies de l'information sur la protection de la vie privée.
- Sensibiliser davantage le public aux technologies ayant une incidence sur la vie privée.
- Fournir une orientation pratique aux organisations sur la mise en œuvre de technologies particulières.

- Sécurité nationale
  - Veiller à ce que les initiatives axées sur la sécurité nationale protègent adéquatement la vie privée.
  - Surveiller adéquatement, chez les organismes chargés de la sécurité nationale, les pratiques de gestion des renseignements personnels et voir à ce que ces organismes se responsabilisent.
  - Sensibiliser le public aux incidences pour la vie privée des initiatives en matière de sécurité nationale.

- Intégrité et protection de l'identité, vol d'identité
  - Améliorer les pratiques de gestion des renseignements personnels des organisations.
  - Sensibiliser le public à la protection de l'identité.
  - Persuader le gouvernement fédéral d'adopter une approche coordonnée en matière de protection de l'identité.

- Information génétique
  - Promouvoir la recherche et les connaissances pour relever les nouveaux défis posés par la génétique dans le contexte des régimes conventionnels de protection des données.
  - Sensibiliser le public aux utilisations possibles de l'information génétique.

Promouvoir la protection mondiale de la vie privée pour les Canadiennes et Canadiens

- Chercher à apporter des modifications à la *LPRPDÉ*; coopérer avec d'autres autorités de protection des données pour s'assurer que les mesures prises pour protéger la vie privée sont complètes et harmonieuses.
- Présider un groupe de bénévoles de l'OCDE chargé d'examiner des moyens d'améliorer la coopération entre les autorités de protection des données et d'autres organes d'application du droit à la vie privée.
- Continuer de travailler avec un groupe de l'APEC axé sur la confidentialité des données qui a élaboré un cadre de protection de la vie privée à l'intention de ses pays membres.

ANNEXE 1 – DÉFINITIONS; PROCESSUS D'ENQUÊTE

DÉFINITIONS DES TYPES DE PLAINTES DÉPOSÉES EN VERTU DE LA *LPRPDÉ*

Les plaintes adressées au CPVP sont réparties selon les principes et les dispositions de la *LPRPDÉ* qui auraient été enfreints :

- **Accès.** Une personne s'est vue refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements ou parce que l'organisation a invoqué des exceptions afin de soustraire les renseignements.

- **Responsabilité.** Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou qu'elle garde ou elle a omis de désigner une personne responsable de surveiller l'application de la Loi.

- **Exactitude.** Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont exacts, complets et à jour.

- **Possibilité de porter plainte.** Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la Loi ou elle a enfreint ses propres procédures et politiques.

- **Collecte.** Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.

- **Consentement.** Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement de la personne concernée ou elle a fourni des biens et des services à la condition que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels.

- **Correction/Annotation.** L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas

de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.

- **Frais.** Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.

- **Conservation.** Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins qu'une organisation a déclarées au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.

- **Mesures de sécurité.** Une organisation n'a pas protégé les renseignements personnels qu'elle détient par des mesures de sécurité appropriées.

- **Délais.** Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la Loi.

- **Utilisation et communication.** Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles pour lesquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la Loi.

DÉFINITIONS DES CONCLUSIONS ET D'AUTRES DISPOSITIONS

Le CPVP a élaboré des définitions de conclusions et de décisions afin d'expliquer les résultats des enquêtes effectuées conformément à la *LPRPDÉ* :

- **Non fondée.** L'enquête n'a pas permis de déceler des éléments de preuves qui suffisent à conclure qu'une organisation a enfreint les droits du plaignant en vertu de la *LPRPDÉ*.

- **Fondée.** L'organisation n'a pas respecté une disposition de la *LPRPDÉ*.

- **Résolue.** L'enquête a corroboré les allégations, mais avant la fin de l'enquête, l'organisation a pris des mesures correctives pour remédier à la situation, à la satisfaction du CPVP, ou s'est engagée à prendre ces mesures.

- **Fondée et résolue.** La commissaire est d'avis, au terme de son enquête, que les allégations semblent fondées sur des preuves, mais fait une recommandation à l'organisation concernée avant de rendre ses conclusions, et l'organisation prend ou s'engage à prendre les mesures correctives recommandées.

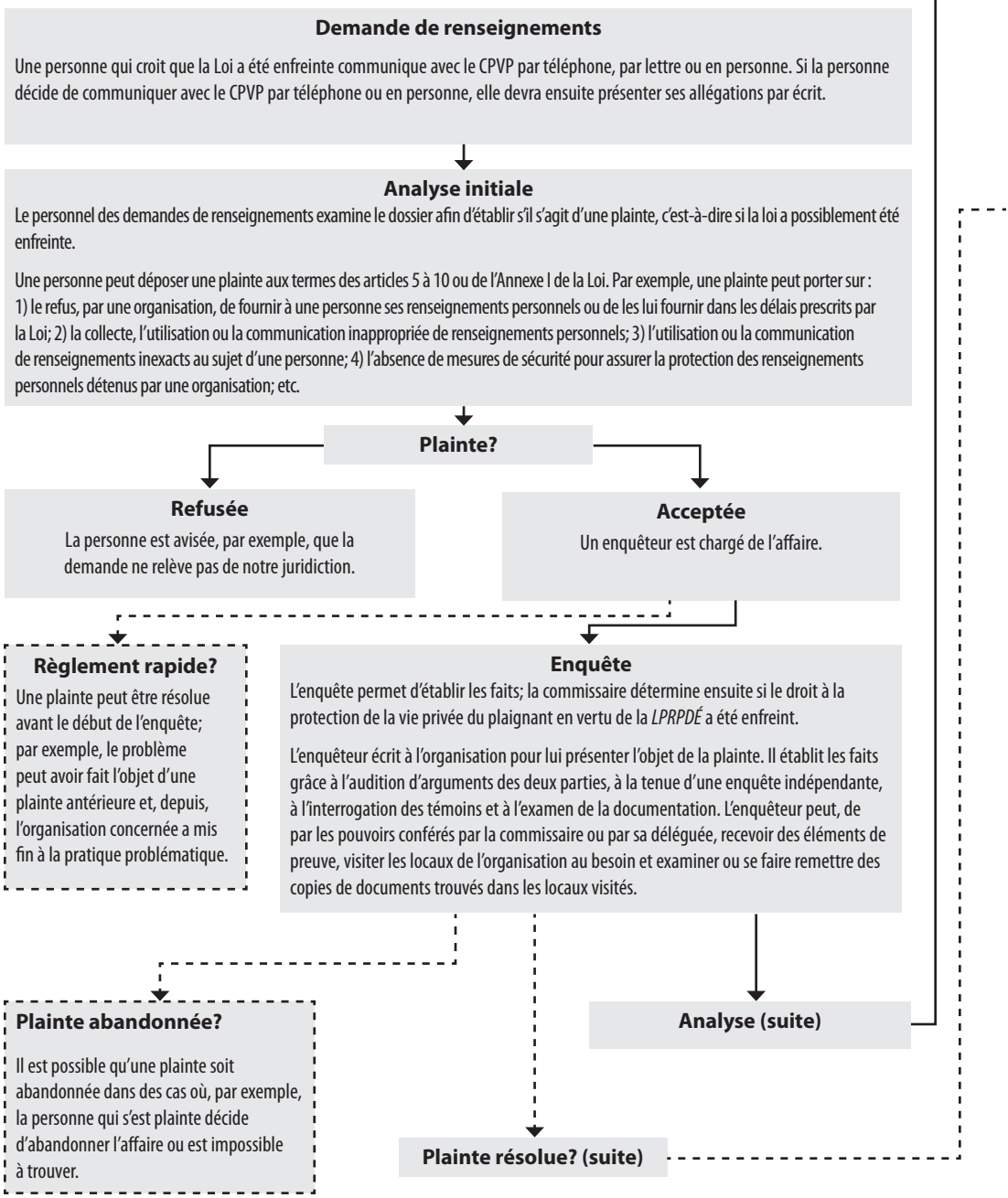
- **Réglée en cours d'enquête.** Le CPVP aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. Aucune conclusion n'est rendue.

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

- **Hors juridiction.** L'enquête a démontré que la *LPRPDÉ* ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.

- **Réglée rapidement.** Situation dans laquelle l'affaire est réglée avant même qu'une enquête officielle ne soit entreprise. À titre d'exemple, si une personne dépose une plainte concernant un sujet qui a déjà fait l'objet d'une enquête par le CPVP et qui a été jugé conforme à la *LPRPDÉ*, nous donnons les explications nécessaires à la personne plaignante. Cette conclusion s'applique également lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du CPVP.

PROCESSUS D'ENQUÊTE EN VERTU DE LA *LPRPDÉ*



Note : une ligne discontinue (- - - -) indique un résultat *possible*.

Analyse

L'enquêteur analyse les faits et formule ses recommandations à l'intention de la commissaire à la protection de la vie privée ou de sa déléguée. Il informe également les parties des recommandations fondées sur l'analyse des faits qu'il remettra à la commissaire ou à sa déléguée. À cette étape, les parties peuvent faire d'autres auditions d'arguments.

Au besoin, des consultations internes sont effectuées avec, par exemple, le concours de la Section des services juridiques ou de la Section de la recherche et des politiques.

Plainte résolue?

Le CPVP cherche à résoudre les plaintes et à prévenir d'autres infractions à la Loi. La commissaire favorise la résolution des différends par l'entremise de la médiation, de la négociation et de la persuasion. L'enquêteur participe au processus.

Conclusions

La commissaire à la protection de la vie privée ou sa déléguée examine le dossier et évalue le rapport. La commissaire ou sa déléguée, et non l'enquêteur, détermine les conclusions à tirer et décide s'il faut présenter des recommandations à l'organisation.

Rapport préliminaire

Si les résultats de l'enquête permettent de conclure qu'il y avait selon toute probabilité infraction à la *LPRPDÉ*, la commissaire à la protection de la vie privée ou sa déléguée recommande à l'organisation des mesures pour remédier au problème et lui demande de lui indiquer dans un délai précis comment elle entend mettre ces mesures en œuvre.

Rapport final et lettre de conclusions

La commissaire ou sa déléguée envoie la lettre de conclusions d'enquêtes aux parties. Cette lettre présente la plainte, les faits établis, l'analyse et la réponse de l'organisation à toute recommandation faite dans le cadre du rapport préliminaire.

Les conclusions possibles sont les suivantes :

Non fondée : La preuve ne permet pas à la commissaire à la protection de la vie privée ou à sa déléguée de conclure que le droit à la protection de la vie privée du plaignant en vertu de la *LPRPDÉ* a été enfreint.

Fondée : L'organisation n'a pas respecté l'une des dispositions de la Loi.

Résolue : La preuve recueillie au cours de l'enquête donne raison au plaignant mais, avant que l'enquête ne soit terminée, l'organisation a pris ou s'est engagée à prendre des mesures pour corriger le problème.

Fondée et résolue : L'enquête donne raison au plaignant, et l'organisation a pris ou s'est engagée à prendre les mesures correctives recommandées dans le rapport préliminaire de la commissaire, au terme de l'enquête.

Dans la lettre de conclusions, la commissaire à la protection de la vie privée ou sa déléguée informe le plaignant de son droit de recours devant la Cour fédérale.

Lorsque des recommandations sont présentées à une organisation, des employés du CPVP effectuent un suivi pour vérifier si elles ont bel et bien été appliquées.

Le plaignant ou la commissaire à la protection de la vie privée peut choisir de demander une audience devant la Cour fédérale. La Cour fédérale a le pouvoir d'ordonner à une organisation de corriger ses pratiques ainsi que de publier un avis énonçant les mesures prises ou envisagées pour corriger ses pratiques. La Cour peut accorder des dommages et intérêts au plaignant, notamment en réparation de l'humiliation subie. Il n'existe pas de plafond pour ces dommages-intérêts.

Note : une ligne discontinue (- - - -) indique un résultat *possible*.

ANNEXE 2 – STATISTIQUES EN MATIÈRE D'ENQUÊTES ET DE DEMANDES DE RENSEIGNEMENTS

Statistiques sur les demandes de renseignements

Notre Section des demandes de renseignements fournit l'un de nos plus importants services aux Canadiennes et Canadiens – la prestation rapide, directe et personnalisée de renseignements sur les enjeux relatifs à la protection de la vie privée. Nous avons reçu près de 8 000 demandes de renseignements liées à la *LPRPDÉ* en 2007.

Au nombre des questions fréquemment soulevées, mentionnons les suivantes : la collecte et l'utilisation des numéros d'assurance sociale; l'accès aux données personnelles détenues par les institutions financières; l'utilisation et la communication de renseignements personnels dans les secteurs des télécommunications et des ventes. Le vol d'identité constitue une autre raison importante pour laquelle les gens communiquent avec nous. Les forces policières conseillent souvent aux personnes qui ont rempli un rapport de police sur un vol d'identité de communiquer avec le Commissariat pour obtenir de plus amples détails.

Nous avons récemment constaté un intérêt accru des organisations à l'égard des questions transfrontalières.

Période allant du 1er janvier au 31 décembre 2007

Demandes de renseignements en vertu de la *LPRPDÉ* reçues par la Section des demandes de renseignements	
Demandes de renseignements téléphoniques	6 428
Demandes de renseignements écrites (lettre et télécopie)	1 208
Nombre total de demandes reçues	7 636

Demandes de renseignements en vertu de la *LPRPDÉ* réglées par la Section des demandes de renseignements	
Demandes de renseignements téléphoniques	6 417
Demandes de renseignements écrites (lettre et télécopie)	1 142
Nombre total de demandes résolues	7 559

PLAINTES REÇUES PAR TYPE DE PLAINTE

Les plaintes reçues en plus grand nombre sont de loin celles qui concernent la façon dont les organisations utilisent et communiquent les renseignements. Les plaignants allèguent le plus souvent que les renseignements sont utilisés et communiqués à des fins autres que celles pour lesquelles on les a recueillis, et qu'ils sont communiqués à des tiers sans le consentement du principal intéressé.

Les plaintes relatives à la collecte concernent habituellement la collecte de renseignements sans le consentement approprié ou la collecte de renseignements non requis pour les fins convenues.

Les plaintes relatives à l'accès concernent essentiellement les allégations selon lesquelles les organisations n'ont pas répondu aux demandes de renseignements personnels ou n'ont pas fourni tous les renseignements auxquels les intéressés croient avoir droit.

Plaintes reçues entre le 1er janvier et le 31 décembre 2007

Type de plainte	Nombre	Pourcentage
Utilisation et communication	120	34
Collecte	68	19
Accès	67	19
Mesures de sécurité	36	10
Consentement	16	5
Délais	13	4
Responsabilité	8	2
Exactitude	7	2
Conservation	7	2
Transparence	4	1
Correction/Annotation	3	1
Frais	1	<1
Total	**350**	

RÉPARTITION PAR SECTEUR

Plaintes reçues entre le 1er janvier et le 31 décembre 2007

Secteur	Nombre	Pourcentage
Institutions financières	105	30
Télécommunications	42	12
Autres	39	11
Ventes	37	11
Assurance	35	10
Transport	28	8
Services professionnels	26	7
Hébergement	21	6
Santé	9	2,5
Services	6	2
Location	2	<1
Total	**350**	

CATÉGORIES

Institutions financières : banques, agences de recouvrement, agences d'évaluation du crédit, fournisseurs de crédit, conseillers financiers

Télécommunications : diffuseurs, câble/satellite, téléphone, téléphone sans fil, services Internet

Autres : écoles privées, bandes autochtones, compagnies de sécurité, enquêteurs privés, etc.

Ventes : concessionnaires d'automobiles, pharmacies, immobilier, vente au détail, magasins

Assurance : assurance-vie et assurance-santé, assurance sur les biens et assurance risques divers

Transport : aérien, terrestre, ferroviaire, maritime

Services professionnels : comptables, avocats

Hébergement : hôtels, locations, condominiums, gestion des biens

Santé : chiropraticiens, dentistes, médecins, physiothérapeutes, psychologues/psychiatres

Services : garderie, coiffeuses, esthéticiennes

Location : location d'autos et autres

PLAINTES RÉSOLUES PAR TYPE DE PLAINTE

Plaintes résolues entre le 1er janvier et le 31 décembre 2007

Type de plainte	Nombre	Pourcentage
Utilisation et communication	162	39
Collecte	80	19
Accès	68	16
Mesures de sécurité	37	9
Consentement	25	6
Délais	11	3
Responsabilité	9	2
Conservation	9	2
Correction/Annotation	7	2
Exactitude	5	1
Transparence	4	1
Autres (représailles)*	2	<1
Frais	1	<1
Total	**420**	

* Nous avons résolu deux plaintes liées à des représailles ou à une dénonciation. L'exécution des mesures entourant les plaintes liées à des représailles est visée par l'article 27.1 de la *LPRPDÉ*. La disposition a pour objet de s'assurer que les organisations ne prennent pas de représailles contre les employés qui ont allégué, de bonne foi, que leur employeur avait enfreint la *LPRPDÉ* ou allait enfreindre la *LPRPDÉ* ou qui ont refusé de faire quelque chose qui aurait été à l'encontre de la Loi. Les représailles peuvent inclure, entre autres, le renvoi, la suspension, la rétrogradation et les mesures disciplinaires.

La commissaire, dans son rôle d'ombudsman, est tenue de faire enquête sur les cas de représailles afin de déterminer si elle doit les signaler au procureur général du Canada en vue d'une éventuelle poursuite judiciaire aux termes du *Code criminel*. Le Commissariat a évalué des plaintes liées à des représailles, mais aucun cas n'a mérité d'être confié au procureur général.

Nombre de plaintes en attente
(en attente d'une attribution à un enquêteur) au 31 décembre 2007 : 44

PLAINTES RÉSOLUES PAR TYPE DE CONCLUSION

Près du tiers de nos plaintes résolues ont été réglées. En d'autres mots, nous avons réussi dans un grand nombre de cas à trouver des solutions qui ont satisfait les plaignants, les parties intimées et le Commissariat.

La deuxième plus grande catégorie est celle des cas abandonnés. Plusieurs raisons peuvent expliquer une telle situation, comme des motifs personnels, parce qu'une organisation a réglé une question avant le début de l'enquête, ou parce que le Commissariat ne peut aller de l'avant étant donné qu'un plaignant ne lui a pas fourni les détails additionnels nécessaires pour réaliser une enquête.

Plaintes résolues entre le 1er janvier et le 31 décembre 2007

Conclusions	Nombre	Pourcentage
Réglée en cours d'enquête	125	30
Abandonnée	89	21
Non fondée	64	15
Fondée et résolue	62	15
Résolue	41	10
Réglée rapidement	14	3
Hors juridiction	14	3
Fondée	9	2
Autres (représailles)	2	<1
TOTAL	**420**	

DÉLAIS DE TRAITEMENT DES ENQUÊTES EN VERTU DE LA *LPRPDÉ* — PAR TYPE DE CONCLUSION

Environ le quart de nos enquêtes sont menées à terme en moins d'un an. Les cas plus complexes demandent davantage de temps. À titre d'exemple, les cas impliquant plusieurs administrations ou nécessitant une recherche exhaustive dans les pratiques industrielles seront habituellement plus longs à régler. Parfois, les cas s'étirent parce que l'information se fait attendre.

Période allant du 1er janvier au 31 décembre 2007

Décision	Délai moyen de traitement en mois
Réglée rapidement	3,36
Abandonnée	11,18
Hors juridiction	12,07
Réglée en cours d'enquête	12,17
Non fondée	20,56
Résolue	20,68
Fondée et résolue	23,15
Fondée	24,36
Autres (représailles)	26,00
Moyenne globale	**15,71**

CONCLUSIONS PAR TYPE DE PLAINTE

Plaintes résolues entre le 1er janvier et le 31 décembre 2007

	Abandonnée	Réglée rapide-ment	Hors juridiction	Non fondée	Autres	Résolue	Réglée	Fondée	Fondée et résolue	TOTAL
Utilisation et communication	26	8	6	27	0	8	46	3	38	**162**
Collecte	18	2	2	18	0	7	25	2	6	**80**
Accès	17	2	5	4	0	15	19	1	5	**68**
Mesures de sécurité	9	1	0	4	0	3	11	1	8	**37**
Consentement	7	1	1	2	0	5	7	0	2	**25**
Délais	4	0	0	0	0	2	3	2	0	**11**
Responsabilité	0	0	0	2	0	1	5	0	1	**9**
Conservation	2	0	0	2	0	0	5	0	0	**9**
Correction/ Annotation	3	0	0	3	0	0	0	0	1	**7**
Exactitude	2	0	0	1	0	0	1	0	1	**5**
Transparence	0	0	0	1	0	0	3	0	0	**4**
Autres	0	0	0	0	2	0	0	0	0	**2**
Frais	1	0	0	0	0	0	0	0	0	**1**
TOTAL	**89**	**14**	**14**	**64**	**2**	**41**	**125**	**9**	**62**	**420**

CONCLUSIONS PAR SECTEUR INDUSTRIEL

Plaintes résolues entre le 1er janvier et le 31 décembre 2007

	Abandonnée	Réglée rapide-ment	Hors juridiction	Non fondée	Autres	Résolue	Réglée	Fondée	Fondée et résolue	TOTAL
Institutions financières	24	5	3	21	0	14	28	0	18	**113**
Télécom-munications	11	2	2	12	1	5	17	4	17	**71**
Ventes	7	3	1	2	0	5	34	0	9	**61**
Autres	17	0	7	8	0	2	23	0	1	**58**
Assurance	13	2	0	3	0	6	11	1	8	**44**
Transport	4	1	0	11	1	4	7	2	3	**33**
Services professionnels	3	1	1	2	0	2	1	2	2	**14**
Services	2	0	0	4	0	1	0	0	4	**11**
Hébergement	7	0	0	0	0	0	2	0	0	**9**
Location	0	0	0	0	0	2	2	0	0	**4**
Santé	1	0	0	1	0	0	0	0	0	**2**
TOTAL	**89**	**14**	**14**	**64**	**2**	**41**	**125**	**9**	**62**	**420**

DÉLAIS DE TRAITEMENT DES ENQUÊTES EN VERTU DE LA *LPRPDÉ* — PAR TYPE DE PLAINTE

Période allant du 1er janvier au 31 décembre 2007

Type de plainte	Délai moyen de traitement en mois
Exactitude	9,4*
Frais	10,0*
Délais	11,3
Conservation	12,7
Accès	14,5
Transparence	15,3*
Correction/Annotation	15,4
Utilisation et communication	15,8
Mesures de sécurité	15,9
Responsabilité	16,2
Collecte	17,0
Consentement	18,0
Autres	26,0*
Moyenne globale	15,7

*Le délai de traitement pour ces types de plaintes se rapporte chaque fois à six cas ou moins.