Commissariat
à la protection de
la vie privée du Canada

Office of the
Privacy Commissioner
of Canada

Une période charnière pour la vie privée

Rapport annuel au Parlement 2021-2022 concernant la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*

Ce document est diffusé sur Internet à l'adresse suivante : www.priv.gc.ca

This document is also available in English.

La version html de ce rapport a préséance sur le présent document en cas de divergence.

Rapport annuel au Parlement 2021-2022 concernant la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*

Commissariat à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec) K1A 1H3

© Sa Majesté le Roi du chef du Canada pour le Commissariat à la protection de la vie privée du Canada, 2022
Numéro de catalogue : IP51-1F-PDF
ISSN : 1913-3375

Table des matières

Message du commissaire 1

La réforme législative : de nouvelles lois à l'horizon 5

La protection de la vie privée en chiffres 9

La *Loi sur la protection des renseignements personnels* : rétrospective de l'exercice 11

- Prestation de services-conseils au gouvernement 12
- Mesures de conformité 20
- Atteintes en vertu de la *Loi sur la protection des renseignements personnels* 27

La *Loi sur la protection des renseignements personnels et les documents électroniques* : rétrospective de l'exercice 31

- Atteintes au titre de la *Loi sur la protection des renseignements personnels et les documents électroniques* 33
- Application de la *Loi sur la protection des renseignements personnels et les documents électroniques* 38
- Activités de l'unité de vérification de la conformité 44
- Conseils et activités de sensibilisation à l'intention des entreprises 45
- Programme des contributions 46

Points saillants des autres travaux menés par le Commissariat 48

- Conseils au Parlement 48
- Coopération avec des autorités canadiennes et étrangères 51
- Devant les tribunaux 57

Annexe 1 : Définitions 64

- Types de plaintes 64
- Décisions 66

Annexe 2 : Tableaux statistiques 68

- Tableaux relatifs à la LPRP 68
- Tableaux relatifs à la LPRPDE 84

Annexe 3 : Lois essentiellement similaires 91

Annexe 4 : Rapport de la commissaire spéciale à la protection de la vie privée 92

Message du commissaire

La protection de la vie privée est à une période charnière. La technologie numérique, de plus en plus axée sur les renseignements personnels, touche tous les aspects de notre vie : depuis les plus complexes, comme la lutte contre une pandémie mondiale et la prévention du crime, jusqu'aux plus simples, comme l'achat d'un café et l'utilisation du téléphone pour communiquer les uns avec les autres.

Au cours des prochaines années, les institutions canadiennes devront trouver les bonnes façons de protéger et de promouvoir notre droit fondamental à la vie privée tout en tirant parti des nouvelles possibilités technologiques. Il s'agit là d'un défi de taille. Pour ce faire, il faudra moderniser les lois fédérales sur la protection des renseignements personnels dans les secteurs public et privé, tant pour réagir et s'adapter à ces changements sociétaux et technologiques que pour suivre le rythme des autres administrations en matière de législation, au Canada comme à l'étranger.

En juin dernier, le gouvernement a franchi une étape importante à cet égard en déposant le projet de loi C-27, la *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, qui vise à moderniser la *Loi sur la protection des renseignements personnels et les documents électroniques*. Ce projet de loi témoigne du fait que le gouvernement reconnaît que les Canadiens ont besoin de lois modernisées sur la protection des renseignements personnels et qu'ils s'attendent à de telles lois. En ma qualité de nouveau commissaire à la protection de la vie privée du Canada, je compte présenter mes observations sur le projet de loi proposé au Parlement cet automne.

Comme je l'ai précisé aux parlementaires lors de l'examen de ma candidature proposée au poste de commissaire, je vais promouvoir et mettre en œuvre une vision qui fait valoir ce qui suit :

1- la protection de la vie privée est un droit fondamental;
2- la protection de la vie privée est un moyen pour favoriser l'intérêt public et appuyer l'innovation et la compétitivité du Canada;
3- la protection de la vie privée est un moyen pour accentuer la confiance des Canadiens envers leurs institutions et un moteur pour la participation et la contribution de ceux-ci à une économie numérique vigoureuse.

Cette vision repose sur le fait que les Canadiens veulent pouvoir participer activement et en toute connaissance de cause au monde numérique, sans être obligés de choisir entre cette participation et leur droit fondamental à la vie privée. Les Canadiens devraient être en mesure de bénéficier des initiatives d'intérêt public et des avancées économiques rendues possibles grâce aux nouvelles technologies, tout en ayant l'assurance que leurs lois et leurs institutions sont là pour protéger adéquatement leurs renseignements personnels. Bref, la protection de la vie privée est fondamentale, elle sert d'importants intérêts publics et privés et permet de susciter la confiance nécessaire.

Pour concrétiser cette vision, nous devrons déployer sans relâche des efforts sur plusieurs fronts : la défense des intérêts, l'application de la loi, la protection, la promotion et la sensibilisation. Le Commissariat ne pourra pas y parvenir seul. C'est pourquoi nous comptons travailler et nouer des relations solides et efficaces avec des intervenants du domaine de la protection des renseignements personnels, des représentants des secteurs public et privé qui sont des champions en la matière ainsi qu'avec nos homologues au pays et à l'étranger.

Le présent rapport annuel donne une vue d'ensemble des importants travaux réalisés par le Commissariat en 2021-2022, soit la dernière année du mandat de mon prédécesseur.

Je profite de l'occasion pour remercier Daniel Therrien, qui a fait preuve d'un leadership exceptionnel au service des Canadiens pendant les huit années où il a occupé les fonctions de commissaire. Il a été un excellent défenseur de la réforme législative et a contribué à mieux faire connaître et comprendre le droit à la vie privée au Canada et dans le monde.

Au cours de la dernière année, le Commissariat a participé à bon nombre d'enquêtes, de travaux d'élaboration de politiques et d'initiatives en collaboration avec les secteurs public et privé, qui revêtent une grande importance. En plus de présenter à la Chambre des communes et au Sénat des mémoires exhaustifs sur la réforme législative, le Commissariat a préparé et commandé des travaux novateurs d'élaboration de politiques pour traiter d'importantes questions ayant des répercussions sur d'autres administrations au pays et à l'échelle internationale.

De bien des façons, qu'il s'agisse de ses processus pour assurer la conformité, de son rôle de chef de file dans des réseaux internationaux de protection de la vie privée, de sa collaboration avec ses homologues au pays ou à l'étranger, ou des services-conseils et documents d'interprétation qu'il offre à des organisations des secteurs public et privé, le Commissariat est une figure de premier plan dans les efforts visant à assurer la protection de la vie privée et à mieux faire connaître et respecter le droit à la vie privée au Canada et dans le monde.

Au nombre des questions qui ont fait l'objet d'une enquête l'an dernier, mentionnons des mesures de lutte contre la pandémie, le recours à la technologie de reconnaissance faciale par les services de police, le suivi des déplacements des clients de Tim Hortons et la surveillance vidéo et audio en continu de chauffeurs de camion. Ces dossiers, où il est question de l'application de la loi, ont démontré une fois de plus les nombreuses formes que peuvent prendre les atteintes à la vie privée des Canadiens causées par la technologie. Ils ont aussi fait ressortir l'importance de mettre rapidement en place des mécanismes efficaces pour cerner et tenir compte dès le départ des préoccupations à ce chapitre.

Le droit à la vie privée et les enjeux connexes touchent tout le monde : les jeunes, les aînés, les personnes qui sont fascinées par la technologie et même celles qui ne le sont pas.

C’est sans aucun doute une période cruciale actuellement pour la protection de la vie privée au Canada, et aussi pour le Commissariat.

Je suis heureux de me joindre – en toute humilité – à une équipe aussi impressionnante à un moment des plus stimulants pour l’organisation. Je me réjouis à la perspective de continuer à servir les Canadiens, cette fois-ci en veillant à protéger et à promouvoir leur droit fondamental à la vie privée. Un droit qui est essentiel à leur autonomie, à leur dignité ainsi qu’à la pleine jouissance des droits et libertés au Canada.

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

Philippe Dufresne

La réforme législative : de nouvelles lois à l’horizon

La réforme législative : de nouvelles lois à l'horizon

Nos récents travaux, qu'ils portent sur le recours à la reconnaissance faciale par les services de police ou sur le suivi par inadvertance de la localisation des clients par l'application mobile de Tim Hortons, entre autres, ont mis encore une fois en évidence les limites des lois actuelles sur la protection des renseignements personnels. Ils ont renforcé notre conviction qu'une réforme législative est nécessaire depuis longtemps.

En juin 2022, nous avons accueilli favorablement le dépôt du projet de loi C-27, *Loi de 2022 sur la mise en œuvre de la Charte du numérique* par le ministre de l'Innovation, des Sciences et de l'Industrie, l'honorable François-Philippe Champagne. Un projet de loi antérieur visant à moderniser la loi sur la protection des renseignements personnels dans le secteur privé était mort au feuilleton au moment du déclenchement des dernières élections fédérales. Cette nouvelle avancée très attendue constitue une étape importante vers l'adoption d'une nouvelle loi qui s'appliquera au secteur privé. Nous avons analysé attentivement le nouveau projet de loi de manière à pouvoir conseiller adéquatement le Parlement cet automne.

Par ailleurs, les propos exprimés par le ministre de la Justice, l'honorable David Lametti, après le dépôt du projet de loi C-27 sont encourageants. Selon lui, non seulement la réforme du cadre de protection des renseignements personnels dans le secteur public devrait suivre bientôt, mais aussi les législateurs prennent des mesures pour harmoniser la législation afin que les lois applicables aux secteurs public et privé soient fondées sur les mêmes principes de protection de la vie privée.

Au 21e siècle, une protection efficace de la vie privée requiert l'adoption de lois fédérales dans les secteurs public et privé qui sont interopérables à l'échelle nationale et internationale et qui confèrent à l'organisme de réglementation des pouvoirs lui permettant d'assurer la conformité. Les lois fédérales doivent favoriser l'innovation responsable, mais dans un cadre législatif solide qui reconnaît, défend et protège le droit fondamental à la vie privée.

Technologie de reconnaissance faciale

En mai 2022, les autorités fédérale, provinciales et territoriales du Canada responsables de la protection de la vie privée ont réclamé que les législateurs élaborent un cadre législatif qui établirait clairement et explicitement les situations où le recours à la technologie de reconnaissance faciale par les services de police peut être acceptable.

Cette déclaration commune faisait suite à une consultation publique sur le recours à la reconnaissance faciale par les services de police, au cours de laquelle nous avons entendu à maintes reprises que les lois actuelles régissant l'utilisation de cette technologie n'offraient pas une protection suffisante contre les risques en cause.

Si la reconnaissance faciale est utilisée de manière responsable, elle peut offrir des avantages considérables, par exemple en contribuant à résoudre des crimes graves, à trouver des personnes disparues et à atteindre des objectifs de sécurité nationale.

Cependant, elle peut aussi s'avérer extrêmement envahissante, permettre la surveillance à grande échelle, produire des résultats biaisés et miner les droits de la personne, y compris le droit de participer librement, sans surveillance, à la vie démocratique.

Dans l'attente de nouvelles mesures législatives, nous avons publié un document d'orientation conjoint pour aider les services de police à s'assurer que toute utilisation de la technologie de reconnaissance faciale est conforme à la loi actuelle, réduit les risques d'atteinte à la vie privée et respecte le droit à la vie privée. Malgré tout, nous gardons espoir que le gouvernement adoptera un cadre législatif qui traitera explicitement des risques associés à cette technologie.

Réforme législative fondée sur les droits

Dans le mémoire sur le projet de loi C-11 que nous avons présenté au Parlement, nous avons recommandé que toute nouvelle loi s'inscrive dans un cadre fondé sur les droits qui reconnaît la protection de la vie privée comme un droit de la personne et en tant qu'élément essentiel à l'exercice d'autres droits fondamentaux.

Certains ont soutenu qu'il n'est pas possible d'adopter une approche fondée sur les droits dans une loi fédérale sur la protection de la vie privée, en invoquant le fait que la protection des renseignements personnels est une question de « droits civils » qui, en vertu de la Constitution, relève de la compétence provinciale.

Nous espérons que l'avis juridique émis par le cabinet Addario Law LLP à la demande du Commissariat et publié par ce dernier en mai dernier atténue ces préoccupations. Selon cet avis juridique, certaines des modifications proposées par le Commissariat auraient comme effet soit de « renforcer » la constitutionnalité de la loi proposée, soit de « n'avoir aucune incidence » sur ce plan.

Préparation en vue de nouvelles lois

Le Commissariat a déjà commencé à travailler à un plan de transition en s'appuyant sur le projet de loi qui a été remplacé par le projet de loi C-27. Il souhaite ainsi s'assurer d'être en mesure d'appliquer rapidement les nouvelles lois protégeant les renseignements personnels une fois qu'elles entreront en vigueur. Dans le cadre de ces travaux, il a effectué l'établissement des coûts, produit une modélisation de la croissance et mené des exercices de planification et de consultation portant sur ses nouvelles responsabilités éventuelles, comme un pouvoir de rendre des ordonnances, un pouvoir en matière d'arbitrage et des obligations liées à l'examen des codes de pratique et des programmes de certification.

Par ailleurs, comme nous en avons fait état dans notre rapport annuel précédent, le ministère de la Justice a publié un document de discussion et de consultation dans lequel il proposait des modifications à la *Loi sur la protection des renseignements personnels.* Mentionnons l'imposition de nouvelles obligations aux ministères en matière d'évaluation des facteurs relatifs à la vie privée (EFVP) ainsi que l'attribution de nombreuses nouvelles responsabilités au Commissariat – notamment celles de donner des orientations aux institutions fédérales et d'entreprendre des activités d'éducation du public.

Nous accueillons favorablement bon nombre des modifications prévues. Cela dit, le nombre d'EFVP que nous recevrons pourrait alors monter en flèche, tout comme le nombre de demandes pour des orientations de la part du secteur public. Nous devrons donc disposer de ressources suffisantes pour répondre à la demande dans des délais raisonnables.

Conclusion

Il ne fait aucun doute que l'économie moderne est de plus en plus dépendante de la valeur des données extraites au moyen des technologies numériques. Toutefois, nous avons aussi constaté les risques inhérents aux technologies qui ne disposent pas de mesures de protection adéquates, et les préjudices qu'elles peuvent causer. Cela nous a amenés à conclure que l'approche à adopter consiste en une réforme de nos lois sur la protection des renseignements personnels de manière à ce qu'elles soient axées sur la reconnaissance et la protection de la vie privée en tant que droit fondamental, et que du même coup, elles servent l'intérêt public, favorisent l'innovation et renforcent la confiance des Canadiens à l'égard de leurs institutions et de l'économie numérique.

Nous sommes optimistes à cet égard : selon nous, un nouveau régime fédéral de protection des renseignements personnels est enfin à portée de main.

Pour en savoir davantage

- Résumé des principales recommandations pour une nouvelle loi fédérale sur la protection des renseignements personnels dans le secteur privé présentées dans le mémoire du Commissariat sur le projet de loi C-11 (4 mai 2022)
- Document d'information : Avis juridique sur la validité constitutionnelle des modifications proposées par le Commissariat à l'ancien projet de loi C-11 (4 mai 2022)

La protection de la vie privée en chiffres

La protection de la vie privée en chiffres

Plaintes en vertu de la LPRP acceptées	906
Plaintes en vertu de la LPRPDE acceptées	427
Rapports d'atteintes à la sécurité des données reçus en vertu de la LPRPDE	645
Plaintes en vertu de la LPRPDE fermées par règlement rapide	303
Plaintes en vertu de la LPRP fermées par règlement rapide	319
Activités de liaison des services-conseils avec le secteur privé	18
Plaintes en vertu de la LPRP fermées à l'issue d'une enquête officielle	474
Plaintes fondées déposées en vertu de la LPRP	81 %
Plaintes en vertu de la LPRPDE fermées à l'issue d'une enquête officielle	55
Plaintes fondées déposées en vertu de la LPRPDE	58 %
Lois, projets de loi et études parlementaires examinées sous l'angle de leurs répercussions sur la vie privée	36
Rapports d'atteintes à la sécurité des données reçus en vertu de la LPRP	463
Évaluations des facteurs relatifs à la vie privée (EFVP) reçues	111
Activités de liaison des services-conseils avec le secteur public	105
Avis donnés à des organisations du secteur public à la suite de l'examen d'une EFVP ou d'une consultation à cet égard	119
Communications de renseignements dans l'intérêt public par les institutions fédérales	747
Comparutions devant des comités parlementaires sur des questions touchant les secteurs privé et public	5
Demandes d'information	7 494
Annonces et communiqués diffusés	39
Allocutions et présentations	34
Gazouillis envoyés	863
Abonnés sur Twitter	19 581
Consultations du site Web	3 193 419
Consultations du blogue	24 058
Publications diffusées	19 923

La *Loi sur la protection des renseignements personnels* : rétrospective de l’exercice

La *Loi sur la protection des renseignements personnels* : rétrospective de l'exercice

Dans le cadre de son travail sous le régime de la *Loi sur la protection des renseignements personnels* (LPRP), le Commissariat a continué de mettre l'accent sur les enjeux liés à la pandémie de COVID-19.

Au moment de la rédaction du présent rapport, plusieurs enquêtes en lien avec la crise de santé publique étaient en cours, dont celles relatives aux plaintes concernant la politique du gouvernement sur la vaccination obligatoire des employés fédéraux, les exigences de vaccination pour les voyageurs ainsi que la collecte et l'utilisation, par le gouvernement, des données sur la mobilité.

Au cours de l'exercice écoulé, en plus de ces enquêtes officielles, la Direction des services-conseils au gouvernement du Commissariat a continué de travailler en étroite collaboration avec des intervenants du secteur public, notamment Santé Canada, l'Agence de la santé publique du Canada (ASPC) et l'Agence des services frontaliers du Canada (ASFC), dans des dossiers liés à la protection de la vie privée dans le contexte de la pandémie de COVID-19. Ces travaux ont donné lieu à des changements dans les activités et les programmes touchant les mesures de contrôle frontalier, la quarantaine ainsi que le traçage et la recherche des contacts. Nous avons également collaboré avec les organismes centraux relativement au respect des programmes de vaccination et fourni des commentaires dans l'évaluation de l'application Alerte COVID de Santé Canada, qui a été mise hors service en juin 2022.

En ce qui concerne les travaux non liés à la pandémie de COVID-19, le Commissariat a publié son premier rapport d'examen conjoint portant sur les communications d'information ayant trait à la sécurité nationale au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) en collaboration avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). Nous reviendrons sur ce rapport plus loin dans la présente section.

Nous avons en outre mené à terme notre consultation auprès de divers intervenants sur la technologie de reconnaissance faciale. Nous avons utilisé l'information recueillie pour mettre la dernière main au document d'orientation sur la protection de la vie privée à l'intention des services de police, que nous avons publié conjointement avec nos homologues provinciaux et territoriaux. Ces travaux faisaient suite au rapport spécial au Parlement que nous avions publié en juin 2021. Ce rapport spécial, dont il est question dans notre rapport annuel 2020-2021, présentait les résultats d'une enquête portant sur l'utilisation, par la Gendarmerie royale du Canada (GRC), de la technologie de reconnaissance faciale pour effectuer des centaines de recherches dans une base de données compilée illégalement par une entreprise commerciale. Nous avons conclu qu'il s'agissait d'une infraction à la *Loi sur la protection des renseignements personnels.*

La section qui suit présente des initiatives clés menées sous le régime de la *Loi sur la protection des renseignements personnels* en 2021-2022, notamment les travaux liés à la pandémie réalisés par la Direction des services-conseils au gouvernement du Commissariat.

Prestation de services-conseils au gouvernement

Le Commissariat a continué de fournir régulièrement des services-conseils à Santé Canada et à l'ASPC relativement aux enjeux liés à la pandémie de COVID-19.

Dès le début de la pandémie, nous avons créé un cadre qui invitait le gouvernement à utiliser les données d'une manière qui servirait l'intérêt public, tout en protégeant la vie privée. Un élément clé de ce cadre consistait à utiliser dans la mesure du possible des données dépersonnalisées ou agrégées. En tant que principe général, nous avons déclaré au cours de la prestation de nos services-conseils que l'utilisation de données dépersonnalisées ou agrégées à des fins de santé publique peut se faire conformément à notre cadre, si des normes techniques adéquates sont adoptées afin de prévenir la réidentification.

Selon la tendance que nous avons observée, les institutions du secteur public ont de plus en plus recours aux technologies et aux données du secteur privé pour élaborer des politiques ou fournir des services gouvernementaux numériques.

Le recours à l'expertise des entreprises pour aider au fonctionnement de l'État fait ressortir la nécessité d'avoir une plus grande uniformité dans les lois applicables aux secteurs public et privé. Les deux secteurs devraient être assujettis à des normes similaires.

Évaluation de l'application Alerte COVID

Le Commissariat a participé à des discussions productives et approfondies avec le gouvernement du Canada concernant Alerte COVID, l'application de notification des expositions à la COVID-19, pendant le développement et après le lancement de celle-ci en juillet 2020.

Au moment du lancement, le Commissariat a appuyé l'utilisation de l'application Alerte COVID en se fondant sur le fait que cette utilisation serait volontaire, que des mesures rigoureuses pour protéger l'identité des utilisateurs seraient en place et que l'efficacité de l'application puisse être démontrée. Nous avons recommandé que la mise en œuvre de l'application fasse l'objet d'une surveillance étroite, et qu'elle soit mise hors service si de nouvelles informations démontrent qu'elle n'est pas ou n'est plus efficace pour atteindre son objectif. Dans le Cadre pour l'évaluation par le gouvernement du Canada des initiatives en réponse à la COVID-19 ayant une incidence importante sur la vie privée, publié par le Commissariat, il est précisé que les mesures portant atteinte à la vie privée qui ont été prises en raison de la pandémie devraient être limitées dans le temps et prendre obligatoirement fin lorsqu'elles ne sont plus nécessaires.

Santé Canada a invité le Commissariat à participer à une évaluation de l'application en 2021-2022. Cette évaluation visait à déterminer si Alerte COVID respectait les principes de protection de la vie privée énoncés dans la déclaration intitulée « Appuyer la santé publique et bâtir la confiance des Canadiens » sur les applications de traçage des contacts atteints de la COVID-19 et autres applications similaires, publiée en mai 2020 par les commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée. En outre, elle portait sur les mécanismes de gouvernance de l'application et avait pour objet de déterminer si celle-ci contribuait efficacement aux efforts pour réduire la propagation de la COVID-19.

Selon cette évaluation, dont les résultats ont été publiés en juin 2022, l'application a contribué à limiter la propagation du virus. Toutefois, il était difficile de quantifier la mesure dans laquelle

elle y a contribué en l'absence d'indicateurs d'efficacité prédéterminés, comme des points de référence, des cibles et des répercussions mesurables sur la santé publique.

L'évaluation a aussi révélé qu'il aurait fallu prendre des mesures plus tôt au cours de la durée de vie de l'application afin d'en déterminer l'efficacité et qu'il faudrait établir des cibles et des objectifs appropriés avant le lancement de toute nouvelle application semblable.

Santé Canada a désactivé l'application en juin 2022. Le ministère a souligné que, compte tenu de l'évolution des mesures de santé publique provinciales liées à la COVID-19 et de la diminution du nombre de tests PCR effectués dans l'ensemble du pays, moins de clés à usage unique ont été émises et, par conséquent, l'application générait moins de notifications d'exposition potentielle, ce qui a entraîné une baisse de l'utilisation d'Alerte COVID. Nous avons accueilli favorablement les conclusions de l'évaluation, qui sont conformes aux principes de nécessité et d'efficacité énoncés dans le Cadre du Commissariat pour l'évaluation par le gouvernement du Canada des initiatives en réponse à la COVID-19 ayant une incidence importante sur la vie privée.

Pour en savoir davantage

- Examen des répercussions sur la vie privée de l'application Alerte COVID (31 juillet 2020)
- Évaluation de l'application canadienne d'avis d'exposition à la COVID-19 (juin 2022)

Améliorations aux frontières en réponse à la pandémie

Les programmes visant à prévenir, à contrôler, à suivre et à endiguer les cas de COVID-19 à la frontière canadienne sont demeurés hautement prioritaires pendant la deuxième année de la pandémie.

Le Commissariat a communiqué régulièrement avec l'ASFC, Immigration, Réfugiés et Citoyenneté Canada (IRCC) et l'ASPC concernant le resserrement des mesures de contrôle aux frontières et la mise en œuvre de nouvelles technologies et méthodes.

Il a fourni des services-conseils à l'ASFC et à IRCC sur l'utilisation de technologies biométriques et de l'analytique avancée, car ces institutions envisageaient d'adapter leurs initiatives liées à la pandémie pour une utilisation à long terme.

Par exemple, le Commissariat a offert des conseils à l'ASFC alors qu'elle souhaite mettre à profit les pratiques limitant les interactions physiques utilisées à la frontière dans le contexte de la pandémie afin de passer à une frontière sans contact dans les années à venir. Il s'agit notamment d'offrir davantage d'options libre-service et de processus sans papier aux postes frontaliers, comme celles présentées ci-dessous.

Déclaration de l'Agence des services frontaliers du Canada faite à l'avance

Ce projet pilote lancé à la fin de 2021 permet aux voyageurs de transmettre à l'ASFC leur déclaration de douane au moyen de la plateforme ArriveCAN avant d'arriver au Canada.

Les recommandations que le Commissariat a formulées à l'ASFC portaient sur les risques éventuels liés à la limitation de la collecte, à l'exactitude et au consentement. L'Agence a

présenté une courte annexe d'EFVP concernant le projet pilote. Nous avons recommandé à l'ASFC de mener une EFVP complète sur l'ensemble de la plateforme ArriveCAN, y compris sur la fonction Déclaration faite à l'avance intégrée à cette plateforme.

Processus de dédouanement dans le cadre de la Chaîne de confiance

Le projet pilote de la Chaîne de confiance a permis de mettre à l'essai un processus de dédouanement pour les voyageurs aériens qui entrent au Canada. Il visait à simplifier l'identification des voyageurs au moyen de l'utilisation de titres de voyage numériques et de données biométriques ainsi qu'à éliminer des interactions en personne aux douanes pour les voyageurs à faible risque.

Les participants au projet pilote utilisaient une application mobile pour transmettre leurs renseignements par voie électronique à l'ASFC afin de lui permettre d'évaluer les risques avant leur arrivée. Ils pouvaient ensuite franchir les points de contrôle douaniers à l'aéroport sans aucune intervention (sauf si nécessaire) par un agent des services frontaliers.

Même si le projet pilote est terminé, l'ASFC a indiqué qu'elle se servira des leçons qu'elle a apprises à l'avenir afin d'orienter son initiative à plus grande échelle de modernisation des programmes pour les voyageurs. Le Commissariat a recommandé que l'ASFC mette soigneusement à l'essai les technologies biométriques et établisse des cadres de responsabilisation internes avant de mettre en œuvre des mesures de contrôle biométriques de plus grande envergure à la frontière. Il a aussi recommandé que le gouvernement communique clairement au public que les produits et services issus de cette initiative sont facultatifs. Cet aspect est essentiel pour obtenir un consentement valable.

Données biométriques et gestion des frontières

En 2021-2022, le Commissariat a aussi fourni des services-conseils à l'ASFC au sujet de la création et de la mise sur pied de son Bureau de la biométrie et de la gestion de l'identité. L'Agence accorde une grande priorité à l'utilisation des données biométriques dans le cadre de la gestion des frontières. Alors qu'elle utilisera davantage ce type de données dans l'ensemble de ses programmes et activités, le Commissariat continuera de lui donner une orientation et des services-conseils sur les risques d'atteinte à la vie privée, notamment les risques relatifs à l'exactitude et le risque d'utilisation à des fins secondaires. Le Commissariat prévoit de formuler des commentaires à l'ASFC sur son cadre visant à régir l'utilisation des données biométriques et il continuera de lui fournir des services-conseils et d'examiner les évaluations de la vie privée portant sur divers éléments de programme.

Initiatives d'Immigration, Réfugiés et Citoyenneté Canada

Dans le même ordre d'idées, en raison des répercussions de la COVID-19, IRCC a concentré ses efforts sur l'innovation technologique et la modernisation de ses activités. En outre, le ministère mettra à profit, dans le cadre de programmes permanents, de nombreux changements apportés en raison de la pandémie. IRCC a consulté le Commissariat concernant ses plans en vue d'aller de l'avant avec un recours accru à la numérisation et à l'analytique avancée des données afin de réduire le délai de traitement des demandes, d'améliorer la prestation des services, de détecter les fraudes et de renforcer la sécurité des programmes.

Le Commissariat a fourni des services-conseils à IRCC concernant des initiatives comme son projet pilote de saisie numérique, qui lui permet d'extraire directement et automatiquement l'information des passeports au moyen d'une technologie de reconnaissance optique, et son projet de services numériques de passeport, qui permet aux intéressés d'utiliser une application Web axée sur l'infonuagique pour renouveler leur passeport en ligne. Ce projet a vu le jour en partie en raison de la montée en flèche du nombre de demandes et de renouvellements de passeports attribuable à la très forte reprise des voyages observée après la pandémie.

Les services-conseils que le Commissariat a fournis au sujet de ces projets visaient à assurer l'exactitude des renseignements personnels, à éviter une collecte excessive et à s'assurer que les fins auxquelles ces renseignements seront utilisés sont clairement définies et bien comprises afin d'obtenir un consentement valable. Le Commissariat a aussi recommandé à IRCC d'évaluer les algorithmes utilisés dans l'analytique des données pour s'assurer qu'ils sont justes et exacts, de surveiller l'efficacité de leur utilisation et de la réévaluer régulièrement.

Autres conseils et activités de sensibilisation à l'intention des institutions fédérales

La Direction des services-conseils au gouvernement, qui fait partie du Secteur des politiques et de la promotion, encourage la conformité à la *Loi sur la protection des renseignements personnels* en donnant aux institutions fédérales une orientation proactive et des conseils pratiques au sujet des risques d'atteinte à la vie privée liés à l'utilisation des renseignements personnels des Canadiens.

L'objectif de cette direction est de s'assurer que les institutions sont autorisées par la loi à utiliser les renseignements personnels à des fins clairement énoncées, que les risques d'atteinte à la vie privée sont éliminés ou atténués avant le lancement des activités et des programmes du gouvernement fédéral, et que la transparence et la responsabilité des institutions en ce qui a trait à l'utilisation, par le gouvernement, des renseignements personnels des Canadiens sont renforcées. La Direction fournit des services-conseils et formule des recommandations à l'issue de l'examen des EFVP qui sont présentées au Commissariat conformément à la *Directive sur l'évaluation des facteurs relatifs à la vie privée* publiée par le Secrétariat du Conseil du Trésor (SCT). Elle fournit aussi des services-conseils aux institutions lors de la conception et de l'élaboration de leurs initiatives, ainsi que par l'entremise de son populaire programme de sensibilisation du public, dans le cadre duquel elle offre des séances en ligne sur divers sujets liés à la protection de la vie privée. La Direction déploie en outre des efforts de sensibilisation de façon ponctuelle auprès des institutions qui sollicitent une orientation. Elle prévoit d'établir un calendrier fixe d'activités de sensibilisation au cours du prochain exercice, espérant que cette nouvelle formule permettra d'augmenter encore plus le nombre de participants, et d'offrir les séances simultanément à plusieurs institutions.

La Direction fournit des services-conseils aux institutions après avoir examiné leurs initiatives, leurs programmes et leurs activités, dont le niveau de risque et la complexité varient et portant sur divers sujets. En 2021-2022, elle a examiné des programmes sur la prestation d'avantages sociaux, le recours à la technologie de reconnaissance faciale dans le contexte de l'application de la loi et du contrôle des frontières, les services gouvernementaux numériques, la vérification de l'identité numérique et les justificatifs d'identité. La Direction reçoit et examine aussi des ententes d'échange de renseignements, d'autres documents institutionnels qui font partie des

cadres ministériels de gestion de la vie privée ainsi que des préavis de communication de renseignements dans l'intérêt public.

La Direction fournit régulièrement des services-conseils au SCT et lui formule des commentaires au cours de l'élaboration de ses politiques, directives et normes se rapportant à l'utilisation des renseignements personnels.

Selon la tendance dont fait état notre dernier rapport annuel, le Commissariat continue d'examiner un grand nombre d'EFVP, de fournir beaucoup de services-conseils et de mener de nombreuses activités de sensibilisation, ce qui indique que ses interventions sont nécessaires et que les institutions fédérales les apprécient. En 2021-2022, le Commissariat a reçu 111 EFVP et a été consulté 105 fois.

La Direction a également mené, à l'intention d'institutions fédérales, 39 séances de sensibilisation portant sur des sujets variés allant de l'élaboration d'une EFVP au respect de la LPRP lors de l'utilisation de la biométrie, de l'intelligence artificielle (IA) et de la surveillance des médias sociaux. Selon nos estimations, plus de 700 fonctionnaires fédéraux des secteurs des politiques ou de l'élaboration des programmes ou du domaine de l'accès à l'information et de la protection des renseignements personnels (AIPRP) ont assisté à ces séances.

Le Commissariat a également reçu 747 préavis de communication de renseignements personnels dans l'intérêt public, ou dans des situations où l'individu concerné en tirerait un avantage certain. Ce nombre cadre avec la tendance du volume généralement élevé de préavis reçus d'institutions fédérales au cours des dernières années (491 en 2020-2021 et 611 en 2019-2020).

L'alinéa 8(2)m) de la LPRP autorise la communication de renseignements personnels dans les cas où, de l'avis du responsable de l'institution, des raisons d'intérêt public justifieraient nettement une éventuelle violation à la vie privée ou la personne concernée en tirerait un avantage certain. Il incombe au responsable de l'institution d'établir si les raisons d'intérêt public ou l'avantage pour l'individu concerné l'emportent sur le droit à la vie privée. Par ailleurs, l'article 37 de la *Loi sur le ministère de l'Emploi et du Développement social* prévoit des autorisations similaires.

Comme à l'habitude, la grande majorité des préavis reçus provenaient d'Emploi et Développement social Canada (EDSC). Il s'agissait notamment de cas où des clients de Service Canada avaient menacé de s'infliger des blessures ou proféré des menaces contre d'autres personnes. En pareil cas, les services de police locaux reçoivent des renseignements personnels pour vérifier le bien-être des personnes concernées ou assurer la sécurité d'autres personnes. EDSC aide aussi les services de police à trouver des personnes disparues et à aviser les proches en cas de décès d'individus.

Comme la *Loi* confère aux institutions le pouvoir discrétionnaire de communiquer ce type de renseignements, le rôle du Commissariat se limite généralement à s'assurer que celles-ci ont bien évalué le bien-fondé de chaque cas. Étant donné que le Commissariat est souvent informé de telles communications après le fait, ce qui est aussi autorisé par la *Loi*, la Direction fournit des services-conseils lorsqu'elle estime qu'ils auront le plus d'effet et offre une orientation de nature générale, afin que les institutions comprennent bien la façon d'appliquer cette disposition. Nous avons mis à jour notre document d'orientation sur les communications dans l'intérêt public sous le régime de la LPRP en ce sens.

En 2021-2022, la Direction a aussi observé une augmentation du nombre d'institutions qui ont manifesté leur intérêt à l'égard de la technologie de reconnaissance faciale. Par exemple, l'Administration canadienne de la sûreté du transport aérien (ACSTA) remplace actuellement ses anciens systèmes de vérification de l'identité aux points d'entrée des zones à accès réglementé dans les aéroports par le système de contrôle d'accès FaceStation. Les employés et les entrepreneurs de l'ACSTA présentent leur visage pour que leur identité soit confirmée au moyen d'un lecteur de reconnaissance faciale. De même, lorsque les postes de déclaration NEXUS du Programme des voyageurs fiables qui avaient recours au balayage de l'iris pour confirmer l'identité ont atteint la fin de leur vie utile, l'ASFC les a remplacés par de nouveaux postes utilisant les données biométriques du visage.

Lorsqu'une institution se munit d'un système de reconnaissance faciale, la Direction lui recommande systématiquement de faire preuve de prudence et lui souligne l'importance de respecter les principes de nécessité et de proportionnalité.

Le rythme des changements technologiques s'est accéléré de façon générale dans l'ensemble du gouvernement. Par exemple, nous avons constaté que le nombre d'applications et de services numériques déployés pour la population canadienne augmente chaque année. Depuis quelques années, la Direction intervient auprès d'institutions fédérales au sujet de leur recours accru à certaines pratiques – utilisation d'identifiants numériques du secteur privé et des administrations provinciales, numérisation complète des dépôts de documents institutionnels, recours à des systèmes de stockage électroniques et utilisation accrue d'applications permettant aux individus d'avoir accès aux services gouvernementaux. La Direction insiste systématiquement sur la nécessité de prendre pleinement en compte les préoccupations concernant la sécurité et la protection de la vie privée, tout en poursuivant les objectifs de facilité d'accès.

Par ailleurs, la Direction a continué de conseiller les institutions fédérales concernant la surveillance des médias sociaux et la collecte de renseignements sur ces plateformes pour les besoins de leurs programmes. Par exemple, nous avons fourni des services-conseils à l'ASFC au sujet de la collecte de renseignements sur des individus dans les médias sociaux et de l'utilisation de ces renseignements pour prendre des décisions concernant l'admissibilité. La Direction a aussi tenu des séances de sensibilisation pour renseigner l'Agence sur la surveillance des médias sociaux et la collecte des renseignements personnels auxquels le public a accès. Elle a en outre examiné l'EFVP reçue de Statistique Canada sur son recours à la surveillance des médias sociaux pour évaluer l'opinion du public au sujet de ses programmes et activités.

L'ASFC a indiqué qu'elle limite la collecte des renseignements à ceux auxquels le public a accès, mais notre Direction des services-conseils au gouvernement a constaté que l'utilisation de renseignements de source ouverte peut tout de même avoir une incidence négative sur la vie privée, plus précisément en ce qui a trait à l'exactitude, à la transparence et à la façon dont les renseignements personnels sont utilisés. La Direction a conseillé à l'Agence d'évaluer en profondeur les risques d'atteinte à la vie privée en lien avec cette pratique et d'élaborer des documents de procédure à l'intention des employés qui font les recherches. Notre Direction compte poursuivre les discussions à ce sujet.

La Direction a également fourni des services-conseils à Statistique Canada au sujet de son utilisation d'une plateforme de surveillance des médias et d'écoute sociale pour rechercher,

surveiller et analyser les tendances dans les médias sociaux et les conversations portant sur les enjeux qui se rapportent aux programmes et aux activités de cet organisme. Elle lui a recommandé d'évaluer régulièrement les rapports produits par cette plateforme de surveillance et d'écoute des médias sociaux afin de s'assurer que l'utilisation de celle-ci est efficace et proportionnelle à l'atteinte des objectifs établis. La Direction a aussi formulé des observations concernant le point de vue de Statistique Canada selon lequel les utilisateurs prolifiques de plateformes de médias sociaux – et, en particulier, les « influenceurs » – ont de faibles attentes en matière de respect de la vie privée quand ils publient leur opinion. D'après ce que la Direction a constaté, le maintien d'une présence publique dans les médias sociaux peut réduire les attentes des utilisateurs à cet égard, mais cela ne signifie pas pour autant qu'ils renoncent entièrement à leur droit à la vie privée pour ce qui est de leurs données. Les renseignements recueillis à partir du domaine public sont considérés comme des renseignements personnels s'ils correspondent à la définition énoncée à l'article 3 de la LPRP. Par conséquent, lorsque ces renseignements sont recueillis par une institution assujettie à cette loi, ils sont protégés en vertu des exigences imposées par celle-ci.

Programme d'utilisation de caméras corporelles de la Gendarmerie royale du Canada

Le Commissariat travaille avec la GRC depuis plus de 10 ans sur des projets pilotes et d'autres initiatives portant sur les caméras corporelles.

D'après nous, les caméras corporelles sont en soi un outil qui porte atteinte à la vie privée, car elles recueillent des images qui permettent d'identifier des individus. Leur utilisation comme outil d'application de la loi est particulièrement sensible. Les caméras corporelles peuvent être utilisées pour favoriser la transparence et la responsabilité des services de police. Cependant, selon nous, les institutions fédérales qui envisagent d'y avoir recours doivent prendre des mesures pour s'assurer que toute utilisation est autorisée par la loi et que les risques d'atteinte à la vie privée sont gérés de façon appropriée.

En juin 2021, nous avons fourni des services-conseils et formulé des commentaires à la GRC au sujet de son projet de politique sur les caméras corporelles et de son système de gestion de la preuve numérique en ce qui a trait au stockage des enregistrements de ces caméras. Nous avons été heureux de constater que la GRC avait pris en compte bon nombre de nos recommandations, si bien que les modifications apportées à la conception de son programme assurent une meilleure protection de la vie privée. Par exemple, la politique de la GRC énonce maintenant plus clairement les critères d'activation des caméras corporelles avant toute interaction avec le public ou toute réponse à un appel de service.

En outre, la GRC a précisé dans sa politique que les policiers peuvent bloquer l'enregistrement vidéo (mais non audio) pour préserver la dignité des individus dans les situations délicates. De plus, nos discussions ont contribué à faire en sorte que la GRC prévoie des dispositions de protection de la vie privée dans ses contrats avec le fournisseur, à la fois pour les caméras corporelles et le système de stockage des enregistrements vidéo.

À l'avenir, nous continuerons de fournir des services-conseils à la GRC pour nous assurer que le déploiement des caméras corporelles à l'échelle nationale pour les policiers de première ligne se fait de manière à continuer de protéger la vie privée le plus possible. Nous constatons que la GRC élabore des processus de caviardage pour protéger l'identité des passants dont les

images sont saisies par ces caméras, mais qui ne sont pas concernés par l'incident. Nous n'avons pas encore eu l'occasion d'examiner et de formuler des commentaires sur le processus de caviardage. Toutefois, nous avons rappelé à la GRC que ses processus devraient être conçus de façon à protéger le mieux possible la vie privée des mineurs, des passants et d'autres individus non ciblés. Nous comptons poursuivre notre travail avec la GRC dans ce dossier important au fur et à mesure que le programme évoluera.

Nous prévoyons de recevoir une EFVP mise à jour au sujet du déploiement national du programme de caméras corporelles, ainsi qu'une nouvelle EFVP sur le système de gestion de la preuve numérique, aux fins d'examen et de recommandations. Par ailleurs, comme d'autres institutions fédérales souhaitent se munir d'un programme de caméras corporelles, nous fournissons des services-conseils au sujet de ces initiatives pour avoir l'assurance que les risques d'atteinte à la vie privée sont gérés de façon appropriée.

Mesures de conformité

Application de la *Loi sur la protection des renseignements personnels*

Questions de conformité sous le régime de la *Loi sur la protection des renseignements personnels*

En 2021-2022, nous avons accepté 906 plaintes déposées en vertu de la LPRP, ce qui représente une hausse de 10 % par rapport aux 827 plaintes acceptées en 2020-2021.

Comme au cours des derniers exercices, un grand nombre de plaintes portaient sur l'accès aux renseignements personnels (27 %) ou mettaient en cause des institutions qui n'avaient pas donné suite à des demandes d'accès dans les délais prévus par la loi (39 %).

Le Service correctionnel du Canada (182) et la GRC (179) demeurent les institutions fédérales visées par le plus grand nombre de plaintes, suivies par l'ASFC (53), le ministère de la Défense nationale (53) et IRCC (49).

Nous avons reçu 463 déclarations d'atteinte à la vie privée, dont la plupart concernaient la perte (278) ou la communication non autorisée (132) de renseignements personnels.

La majorité des déclarations, plus précisément 93 % d'entre elles, étaient liées à une erreur humaine. Par exemple, des employés avaient envoyé par erreur des renseignements personnels par courriel ou par la poste à la mauvaise adresse, mal géré des données ou des documents en utilisant une solution ou un raccourci inapproprié, perdu des renseignements ou bien les avaient stockés au mauvais endroit. Il y a donc lieu de croire que les politiques ou les procédures de sécurité adoptées par l'institution en question n'ont peut-être pas été suivies ou appliquées.

Ces types d'atteintes à la vie privée montrent qu'il ne suffit pas de mettre en place des politiques et des directives pour protéger les renseignements personnels. Les politiques et les directives sont efficaces uniquement si elles sont mises en œuvre et suivies fidèlement. Il est essentiel que les renseignements personnels soient gérés correctement tout au long de leur cycle de vie – au moment de la collecte, de l'utilisation et du retrait. À cette fin, la sensibilisation et la mobilisation des employés sont cruciales.

Nous sommes toujours préoccupés par le fait que les institutions du secteur public ne déclarent que très peu de cyberattaques, y compris les attaques par maliciel et par hameçonnage. Nous avons reçu cinq déclarations de cyberattaques en 2021-2022, c'est-à-dire neuf déclarations de moins que l'année précédente.

Arriéré de plaintes

Entre avril 2019 et mars 2021, nous avons réussi à mettre à profit une augmentation budgétaire temporaire et à réaliser des gains d'efficacité pour réduire de plus de 90 % notre arriéré de dossiers d'enquête remontant à plus de 12 mois (passant de 324 dossiers en 2019 à 29 à la fin de 2020-2021).

La réduction de l'arriéré et les améliorations apportées à nos processus, notamment le gain d'efficacité technologique, nous ont permis de réduire considérablement le délai de traitement

moyen pour les enquêtes menées sous le régime de la LPRP à 6,17 mois (comparativement à 9,66 mois en 2020-2021). Le temps nécessaire pour mener à bien les enquêtes en vertu de la LPRPDE est passé à 7,8 mois, comparativement à 12,2 mois un an plus tôt.

Toutefois, vu que le financement temporaire a pris fin au cours du présent exercice, l'arriéré de dossiers est remonté à 102 à la fin de mars 2022, ce qui représente 15 % de toutes les enquêtes en cours en vertu de la LPRP ou de la LPRPDE. Même si un arriéré d'environ 15 % est à prévoir compte tenu de nos ressources actuelles, il y a un risque que celui-ci continue à augmenter. Nous continuons donc à réaliser de nouveaux gains d'efficacité en l'absence de financement. La pression attribuable à l'augmentation du nombre de plaintes est amplifiée par l'entrée en vigueur du Décret d'extension nº 3 de la *Loi sur la protection des renseignements personnels*, qui confère aux ressortissants étrangers le droit de demander l'accès à leurs renseignements personnels.

Enquêtes portant sur des plaintes pour non-respect des délais d'accès

L'approche que nous adoptons dans le cadre des enquêtes menées à la suite d'une plainte mettant en cause une institution fédérale qui aurait refusé au plaignant d'avoir accès dans un certain délai aux documents qui le concernent illustre les gains d'efficacité que nous avons réalisés. Cette approche a continué d'accélérer considérablement nos processus d'enquête.

Nous avons été en mesure de réduire à un peu moins de trois mois le délai de traitement des plaintes pour non-respect des délais d'accès.

Selon notre approche actuelle, si une institution fédérale ne permet pas à un plaignant d'avoir accès dans un certain délai aux documents qui le concernent, le Commissariat conclura qu'il y a « présomption de refus ». Cette approche incite les institutions à répondre aux demandes d'accès dans un délai plus raisonnable et confère aux plaignants le droit de porter l'affaire devant la Cour fédérale lorsqu'elles ne le font pas.

Durée de traitement dans les enquêtes relatives aux délais

Exercice	Délai de traitement moyen, en mois
2021-2022	2,91
2020-2021	5,04
2019-2020	7,50
2018-2019	6,98
2017-2018	6,28

Au cours de la dernière année, nous nous sommes aussi préparés à l'incidence du Décret d'extension nº 3 de la *Loi sur la protection des renseignements personnels*, qui est entré en vigueur le 13 juillet 2022. Auparavant, seuls les citoyens canadiens et les personnes se trouvant physiquement au Canada avaient le droit d'accéder aux renseignements personnels détenus à leur sujet par les institutions fédérales.

Le Décret d'extension autorise les ressortissants étrangers qui se trouvent à l'extérieur du Canada à présenter une demande d'accès à leurs renseignements personnels et, par

conséquent, à déposer une plainte si on leur refuse cet accès. En prévision de l'entrée en vigueur de ce décret, les institutions fédérales, principalement IRCC, prévoyaient de recevoir des centaines de milliers de nouvelles demandes de renseignements personnels. Elles s'attendaient, par effet de domino, à une augmentation du nombre de plaintes déposées au Commissariat. Nous avons donc cherché des solutions de financement et mis au point de nouvelles méthodes d'enquête afin d'atténuer les effets de cette augmentation.

Règlement rapide

Notre direction des admissions, du règlement et de la conformité, dont fait partie l'équipe de la réception et du règlement rapide des plaintes, est chargée de s'assurer que les plaintes non systémiques sont résolues aussi efficacement que possible.

Le règlement rapide – méthode d'enquête reposant sur la négociation ou l'arbitrage – constitue généralement le résultat optimal pour les parties concernées. En pareil cas, le Commissariat ne publie aucun rapport de conclusions d'enquête. Le règlement rapide continue de faire partie intégrante de nos activités.

Pourcentage des plaintes fermées par règlement rapide

Exercice	Pourcentage des plaintes fermées par règlement rapide
2021-2022	40 %
2020-2021	52 %
2019-2020	25 %
2018-2019	32 %
2017-2018	37 %

Le pourcentage des plaintes fermées strictement par règlement rapide, qui se chiffre à 40 % en 2021-2022 est en baisse par rapport au sommet de 52 % atteint en 2020-2021. Soulignons que l'équipe du règlement rapide produit aussi des rapports d'enquête sommaires à l'issue d'enquêtes dans des dossiers relativement simples, qui se soldent par la publication d'un bref rapport ou d'une lettre de conclusions. Grâce au règlement rapide et aux enquêtes sommaires, cette équipe a fermé 88 % de toutes les plaintes déposées en vertu de la LPRP, incluant celles pour non-respect des délais d'accès.

Résumé des examens et enquêtes clés

Examen conjoint, avec l'OSSNR, des communications d'information sous le régime de la LCISC

En décembre 2021, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et le Commissariat ont mené à terme leur premier examen conjoint des communications d'information ayant trait à la sécurité nationale au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC). Cet examen a révélé

que 212 des 215 communications faites par des institutions fédérales respectaient les exigences de la LCISC.

Le Service canadien du renseignement de sécurité (SCRS) et le Centre de la sécurité des télécommunications (CST) ont été les principaux destinataires de l'information communiquée au titre de la LCISC en 2020. Avec 159 communications, dont bon nombre concernaient des renseignements contenus dans les demandes de passeport, IRCC est l'institution qui se trouvait à l'origine du plus grand nombre de communications d'information.

Trois communications faites par la GRC ont suscité des préoccupations, en particulier une communication des renseignements personnels de milliers de personnes. Dans ce cas, la GRC a communiqué au ministère de la Défense nationale (MDN) et aux Forces armées canadiennes (FAC) les renseignements biométriques de milliers d'hommes, de femmes et d'enfants détenus par une entité étrangère parce qu'ils étaient soupçonnés d'être membres ou partisans d'une organisation terroriste.

L'examen a fait état de préoccupations à l'égard de cette communication, car la GRC avait alors communiqué des renseignements très sensibles en s'appuyant sur des données incomplètes. L'information manquante aurait été requise pour bien évaluer à la fois l'incidence sur le droit à la vie privée et la communication raisonnablement nécessaire dans les circonstances, comme l'exige la LCISC. Nous nous inquiétions du fait que la GRC ait rejeté la principale conclusion selon laquelle elle ne s'était pas conformée aux exigences de la LCISC dans ce cas.

À la lumière de leur examen conjoint, l'OSSNR et le Commissariat avaient recommandé à la GRC de fournir au MDN et aux FAC des renseignements supplémentaires concernant les données biométriques. Dans sa réponse à notre rapport sur les communications d'information au titre de la LCISC, le gouvernement fédéral n'a pas précisé si la GRC l'avait déjà fait ou allait le faire. Il a plutôt réitéré la défense invoquée par cette institution à l'égard de la communication initiale, qui reposait sur des données incomplètes.

En tout, l'OSSNR et le Commissariat ont formulé 11 recommandations visant à améliorer la conformité des institutions à la LCISC. Ces recommandations portent, par exemple, sur la conservation des documents, la gouvernance et les mesures à prendre pour assurer le respect du critère de communication défini dans la LCISC.

Importance de l'examen des communications au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*

La LCISC autorise les institutions à communiquer de l'information ayant trait à la sécurité nationale, y compris des renseignements personnels, à un groupe restreint d'institutions fédérales dont le mandat porte sur la sécurité nationale.

Cette loi vise à atteindre un équilibre raisonnable entre la vie privée et la sécurité nationale. Une préoccupation importante dans l'élaboration de la LCISC était le risque auquel sont exposés les citoyens respectueux des lois lorsque les renseignements personnels d'« un grand nombre » d'entre eux sont communiqués afin d'identifier « un petit nombre » de personnes réellement impliquées dans des activités préoccupantes pour la sécurité nationale.

Pour en savoir davantage

- Communiqué : L'examen conjoint des communications d'information au titre de la LCISC révèle une conformité en général, mais soulève certaines préoccupations (22 février 2022)

Le ministère de la Défense nationale n'a pas respecté son engagement de confidentialité envers un employé qui a déposé une plainte pour violence en milieu de travail

Le Commissariat a reçu une plainte déposée par un employé du MDN. Selon le plaignant, le Ministère n'avait pas respecté son engagement à préserver son anonymat relativement à une plainte pour violence en milieu de travail qu'il avait déposée.

Le MDN avait transmis des copies du rapport d'enquête sur la plainte pour violence en milieu de travail à des personnes dont le nom ne figurait pas sur un « formulaire connexe de consentement à communiquer l'identité » signé par le plaignant. En signant ce formulaire, l'employé s'attendait à un engagement ferme de la part du Ministère à assurer la confidentialité de l'enquête portant sur sa plainte. Contre toute attente, les renseignements ont été communiqués à des intervenants du domaine des relations de travail et à un deuxième enquêteur chargé d'un dossier similaire.

Le MDN a affirmé que la communication des renseignements personnels était nécessaire pour répondre aux allégations soulevées contre le plaignant, qu'elle n'était pas interdite par le formulaire de consentement en question et qu'elle constituait « un usage compatible ». La LPRP autorise la communication de renseignements sans le consentement de l'individu s'il s'agit d'une communication « aux fins auxquelles ils ont été recueillis […] ou pour les usages qui sont compatibles avec ces fins ».

Notre enquête a révélé que la première communication, aux intervenants du domaine des relations de travail, constituait un usage compatible. En raison du rôle important que jouent les agents des relations de travail, à titre de conseillers en gestion de problèmes en milieu de travail, il est raisonnable de s'attendre à ce qu'un rapport d'enquête sur la violence en milieu de travail leur soit transmis en interne.

Toutefois, compte tenu du libellé du formulaire de consentement, qui suscitait une attente de confidentialité, nous estimons qu'un plaignant dans un processus portant sur la violence en milieu de travail ne s'attendrait raisonnablement pas à ce qu'un rapport d'enquête sur sa plainte serve de preuve dans des procédures disciplinaires distinctes. Nous avons donc conclu que la communication à l'enquêteur ne constituait pas un usage compatible et que cet aspect de la plainte était fondé.

Pour qu'une communication constitue un « usage compatible » autorisé sous le régime de la LPRP, elle doit avoir un lien suffisamment direct avec la fin pour laquelle les renseignements ont été obtenus à l'origine de sorte qu'une personne puisse raisonnablement s'attendre à ce que ceux-ci soient utilisés de cette manière. Il doit y avoir concordance manifeste entre, d'une part, la façon dont les limites de la confidentialité sont expliquées aux intéressés et, d'autre part, le moment où les communications sont faites et la façon dont on procède alors en réalité afin de réaliser des fins valables.

Nous avons recommandé au MDN de modifier les produits ou les outils utilisés par le personnel, ou fournis aux participants, dans un dossier de violence en milieu de travail pour s'assurer que toute communication de renseignements personnels faite pour les besoins d'un « usage compatible » est conforme aux attentes raisonnables d'un participant.

Dans les neuf mois suivant la publication de notre rapport, le MDN a accepté nos recommandations. Il s'est alors engagé à soumettre ses produits et ses outils à l'examen du Commissariat avant d'y mettre la dernière main.

Pour en savoir davantage

- Le MDN a enfreint la *Loi sur la protection des renseignements personnels* en divulguant l'identité d'un plaignant de violence en milieu de travail qui s'attendait à ce que son identité soit confidentielle

Activités de l'unité de vérification de la conformité

Nous formulons souvent des recommandations aux institutions dans nos rapports d'enquête. Notre unité de vérification de la conformité fait le suivi auprès des institutions fédérales pour vérifier si elles mettent en œuvre avec succès nos recommandations. Nous pouvons ainsi nous assurer que les institutions fédérales respectent les engagements qu'elles ont pris envers le Commissariat et les Canadiens.

L'unité de vérification de la conformité fait un suivi des enjeux liés à la LPRP et à la LPRPDE.

En 2021-2022, sept cas de plaintes concernant le secteur public ont été acheminés à l'unité de vérification de la conformité et demeurent ouverts. Il s'agissait entre autres de plaintes contre IRCC, le Service correctionnel du Canada (SCC), la GRC et l'École de la fonction publique du Canada. Dans ces cas, cette unité a joué un rôle actif auprès de l'institution et a donné une rétroaction, au besoin.

La GRC a mis en œuvre les recommandations formulées à l'issue de l'enquête portant sur le recours à la technologie de reconnaissance faciale

En 2021, le Commissariat a déposé un rapport spécial au Parlement à l'issue de son enquête sur l'utilisation, par la GRC, de la technologie de reconnaissance faciale de Clearview AI.

Selon notre enquête, la GRC n'a pas évalué correctement les risques potentiels de manquement à la *Loi* que l'utilisation de l'énorme base de données de Clearview et de la technologie de reconnaissance faciale présentait manifestement. De plus, l'organisation n'a pas de système en place pour assurer le suivi, analyser, examiner et contrôler cette nouvelle méthode de collecte de renseignements personnels. Nous avons donc recommandé à la GRC de mettre en place des mesures systémiques et d'offrir une formation pertinente afin de s'assurer que la collecte des renseignements personnels est limitée comme le prévoit la *Loi*. Ces recommandations s'appliquent à toute nouvelle technologie donnant lieu à la collecte ou à l'utilisation de renseignements personnels.

Bien que la GRC n'ait pas souscrit à certaines de nos conclusions, selon lesquelles nous estimons qu'elle avait contrevenu à la *Loi*, elle a néanmoins accepté de mettre en œuvre nos recommandations.

En créant son Programme national d'intégration des technologies, la GRC a réalisé des progrès considérables sur le front de l'exécution de ses engagements. Depuis le lancement de ce programme, l'équipe responsable a reçu de nombreuses demandes d'évaluation de diverses technologies. La GRC est ainsi bien placée pour respecter l'esprit de nos recommandations.

Au moment de la rédaction du présent rapport, les difficultés au chapitre du budget et de la dotation en personnel risquaient d'empêcher la GRC de rendre ce programme pleinement opérationnel.

Cela dit, la GRC a travaillé en étroite collaboration avec notre équipe de vérification de la conformité. En plus de demander des services-conseils et de la rétroaction à cette dernière sur les mesures prévues, elle a produit des rapports et donné des précisions sur la mise en œuvre des recommandations jusqu'à présent. Nous ferons le point à cet égard dans le prochain rapport annuel.

Pour en savoir davantage

- Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée – Rapport spécial au Parlement sur l'enquête réalisée par le Commissariat à la protection de la vie privée du Canada sur l'utilisation par la GRC de la technologie de Clearview AI et version préliminaire d'un document d'orientation conjoint à l'intention des services de police qui envisagent d'avoir recours à la technologie de reconnaissance faciale (10 juin 2021)
- Enquête conjointe sur Clearview AI, Inc, par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta (2 février 2021)

Atteintes en vertu de la *Loi sur la protection des renseignements personnels*

Dans le secteur public, la déclaration des atteintes à la vie privée est obligatoire en vertu de politiques; dans le secteur privé, elle l'est en vertu de la loi. Le Commissariat demeure préoccupé par les pratiques concernant la déclaration de ces atteintes dans le secteur public.

En raison de la fluctuation du nombre de déclarations d'atteinte à la vie privée faites au cours des cinq dernières années, le risque de sous-déclaration par les institutions fédérales demeure très préoccupant.

Le nombre de déclarations faites par les institutions fédérales est passé de 280 en 2020-2021 à 463 en 2021-2022, ce qui représente une augmentation de 65 %.

Or, cette augmentation découle probablement des nouvelles activités de sensibilisation à la protection de la vie privée et des procédures de déclaration mises en place à EDSC. Ce ministère a fait 349 déclarations d'atteinte au Commissariat en 2021-2022, soit une hausse de 185 par rapport aux 164 déclarations qu'il avait faites en 2020-2021. EDSC est à l'origine de 75 % des déclarations que nous avons reçues au cours du dernier exercice. Avec 36 déclarations, le SCC arrive au deuxième rang pour le nombre de déclarations faites au Commissariat en 2021-2022. Soulignons qu'il s'agit de deux grandes institutions qui traitent une quantité considérable de renseignements personnels.

Comme nous l'indiquions dans nos rapports annuels précédents, il est préoccupant de constater que plusieurs grandes institutions fédérales – dont bon nombre qui traitent une quantité considérable de renseignements personnels ou très sensibles – brillent par leur absence dans l'ensemble des rapports d'atteinte que nous recevons. Seulement 31 des 288 institutions fédérales assujetties à la LPRP nous ont déclaré une atteinte à la vie privée au cours du dernier exercice financier.

Autrement dit, au moins 257 institutions assujetties à la *Loi* n'ont déclaré aucune atteinte l'année dernière.

Si l'on fait abstraction des déclarations faites par EDSC et le SCC, le Commissariat n'a reçu que 78 déclarations faites par des institutions assujetties à la *Loi*. Cette situation est d'autant plus préoccupante que de nombreuses grandes institutions traitent une quantité considérable de renseignements personnels concernant les fonctionnaires fédéraux et la population.

Ce qui est encore plus inquiétant, c'est que 93 % des déclarations d'atteinte reçues par le Commissariat en 2021-2022 sont attribuables à une erreur humaine. Cette forte proportion fait ressortir la nécessité pour les institutions de mettre en œuvre des mesures de protection appropriées et de renforcer la sensibilisation à la protection de la vie privée afin de s'assurer de faire connaître aux employés les politiques et les procédures en place ainsi que leurs responsabilités aux termes de la *Loi*. Il s'agit là de mesures essentielles pour que les institutions soient tenues de rendre des comptes au sujet des renseignements personnels qu'elles recueillent, utilisent ou communiquent.

En outre, comme nous l'avons souligné au cours des exercices précédents, nous continuons de recevoir très peu de déclarations d'atteinte, de la part d'institutions fédérales, qui font état de cyberattaques, et ce, malgré les reportages dans les médias selon lesquels la fréquence et la

gravité de ces incidents augmentent partout dans le monde. Nous n'avons reçu que cinq déclarations de cette nature en 2021-2022, par rapport à neuf au cours de l'exercice précédent. Nous demeurons préoccupés par le fait que le nombre de déclarations de cyberattaque reçues par le Commissariat demeure faible, surtout si on établit une comparaison avec les déclarations d'atteinte en vertu de la LPRPDE : 45 % d'entre elles mettaient en cause des cyberattaques.

Dans certains cas, nous menons des enquêtes sur des atteintes à la vie privée, dont celles qui sont causées par des cyberattaques. Au moment de la rédaction du présent rapport, en plus de l'enquête sur l'ASFC dont nous faisons état dans la prochaine section, le Commissariat poursuivait celle qui porte sur la cyberattaque menée contre le système cléGC utilisé par une trentaine de ministères et organismes fédéraux.

Dans d'autres cas, l'unité responsable des déclarations d'atteinte au Commissariat examine les déclarations reçues sans mener d'enquête formelle. Elle fait alors appel à l'institution concernée et analyse les causes de l'atteinte, cherche à comprendre l'incidence de celle-ci et détermine les mesures à prendre pour atténuer tout préjudice que pourraient subir des individus en raison de cette atteinte et pour éviter que la situation ne se reproduise.

Dans le cadre de ces examens, nous avons remarqué certaines tendances. Par exemple, nous constatons de plus en plus d'atteintes causées par des cyberattaques qui touchent à la fois les secteurs public et privé. Trois des cinq déclarations reçues par le Commissariat en 2021-2022 concernaient des entreprises du secteur privé qui fournissent des services aux institutions fédérales. Comme nous avons aussi constaté une augmentation des enjeux relatifs à la protection de la vie privée dans les partenariats entre les secteurs public et privé, nous sommes d'avis que les institutions gouvernementales devraient porter une plus grande attention aux modalités relatives à la sécurité dans leurs ententes avec leurs fournisseurs de services.

Nous avons également observé que faire appel aux spécialistes de la TI et de la sécurité est souvent essentiel pour garantir une évaluation complète de tout accès non autorisé ou de toute communication de renseignements personnels.

Ces considérations pourraient expliquer le faible taux de déclaration des atteintes liées à des cyberattaques dans le secteur public fédéral, par exemple dans les cas où la responsabilité de déclaration obligatoire des atteintes ou les répercussions de celles-ci ne sont pas bien comprises.

Afin d'assurer une plus grande constance dans la déclaration des atteintes par les institutions fédérales, nous réclamons encore une fois la déclaration obligatoire des atteintes à la vie privée sous le régime de *Loi sur la protection des renseignements personnels* afin de remédier au faible taux de déclaration, un problème systémique dans le secteur public fédéral.

Des images de plaques d'immatriculation captées aux postes frontaliers sont publiées sur le Web invisible après qu'un entrepreneur de l'Agence des services frontaliers du Canada ait été victime d'une atteinte

Le Commissariat a pris l'initiative d'une plainte à la suite de reportages dans les médias qui faisaient état d'une cyberattaque qui visait un entrepreneur auquel avaient recours l'ASFC et la US Customs and Border Protection. L'atteinte mettait en cause des fichiers qui ont été transférés du réseau de l'entrepreneur et publiés dans le Web invisible.

En 2019, l'ASFC a informé le Commissariat que l'atteinte concernait environ 9 000 images de plaques d'immatriculation prises lorsque des voyageurs sont entrés au Canada par le poste frontalier de Cornwall, en Ontario.

Notre enquête visait à déterminer l'incidence de l'atteinte sur les voyageurs entrant au Canada et à évaluer les mesures prises par l'ASFC pour garantir que des mesures de sécurité adéquates étaient en place.

L'enquête a révélé que le nombre d'images de plaques d'immatriculation compromises dans l'atteinte était beaucoup plus élevé que ce qui avait été déclaré au départ, soit près de 1,4 million d'images de plaques. De ce nombre, environ 11 000 ont été publiées dans le Web invisible.

Notre enquête a aussi mis en évidence un manque de cohérence dans la façon dont l'ASFC gérait les données sur les plaques d'immatriculation ainsi que l'absence de mesures de sécurité, notamment de clauses contractuelles suffisantes lui permettant de s'assurer que son partenaire du secteur privé protège adéquatement les renseignements qui lui sont confiés.

Entre autres, le Commissariat a recommandé à l'ASFC de revoir le contrat conclu avec son fournisseur de services pour préciser clairement que les données sur les plaques d'immatriculation constituent des renseignements personnels et que des mesures de protection appropriées s'imposent en matière de conservation, d'utilisation, d'accès et de destruction.

Notre enquête a permis de conclure que la plainte était fondée. Compte tenu de la réponse de l'ASFC et du fait qu'elle a accepté nos recommandations, nous considérons que la plainte est résolue.

Une importante leçon a été tirée de cette affaire : les obligations en matière de protection de la vie privée s'appliquent aussi bien aux renseignements personnels traités par une institution qu'à ceux traités par un entrepreneur agissant en son nom. En pareil cas, la protection de la vie privée est une responsabilité partagée. De plus, il est essentiel que les institutions établissent si les données traitées par un entrepreneur constituent des renseignements personnels et qu'elles le précisent dans les contrats.

Pour en savoir davantage

- Enquête portant sur une atteinte aux renseignements personnels détenus par un entrepreneur de l'Agence des services frontaliers du Canada

La *Loi sur la protection des renseignements personnels et les documents électroniques* : rétrospective de l’exercice

La *Loi sur la protection des renseignements personnels et les documents électroniques* : rétrospective de l'exercice

Les enquêtes que nous avons menées en 2021-2022 sous le régime de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ont donné lieu à des initiatives d'application de la loi fructueuses menées en collaboration avec des homologues canadiens et étrangers. Ces initiatives nous ont donné l'occasion de nous pencher sur les préoccupations relatives à la protection de la vie privée en ce qui concerne les nouvelles technologies.

Par exemple, le Commissariat et ses homologues du Québec, de l'Alberta et de la Colombie-Britannique ont mené à terme une enquête sur l'application mobile de Tim Hortons ainsi que sur la collecte, l'utilisation et la communication, par l'entreprise, des données de géolocalisation des utilisateurs. Nous avons constaté que Tim Hortons avait enfreint les lois sur la protection des renseignements personnels en recueillant de grandes quantités de données de géolocalisation de nature sensible au moyen de l'application.

Comme il en est question dans d'autres sections du présent rapport, nous avons aussi effectué d'importants travaux portant sur l'intelligence artificielle et les technologies de reconnaissance faciale. Mentionnons entre autres une initiative chapeautée par l'Assemblée mondiale pour la protection de la vie privée qui visait à élaborer des principes et des exigences relativement à l'utilisation de renseignements personnels dans les technologies de reconnaissance faciale.

Certaines enquêtes mises en lumière dans la présente section illustrent l'importance d'examiner et de tenir compte des enjeux relatifs à la protection de la vie privée avant de mettre en œuvre de nouvelles technologies. Par exemple, nous avons fait enquête sur une plainte déposée à propos du programme d'authentification biométrique à empreinte vocale d'une entreprise de télécommunications. Nous avons aussi fait enquête sur des plaintes déposées concernant les technologies de surveillance utilisées par deux entreprises de services de transport.

Les travaux que nous avons menés sous le régime de la LPRPDE ont aussi porté en grande partie sur les atteintes à la vie privée qui résultent de cyberincidents mettant en cause des identifiants compromis. Certains des incidents les plus sérieux cités dans les déclarations d'atteinte à la vie privée reçues par le Commissariat concernaient le piratage, des maliciels et l'hameçonnage.

Fait à signaler : le nombre total d'atteintes à la vie privée déclarées au Commissariat a nettement diminué. En fait, il s'agit de la première année depuis novembre 2018 (date d'entrée en vigueur de la déclaration obligatoire) pour laquelle le nombre de déclarations présentées à notre organisme a diminué par rapport à celui de l'année précédente. De surcroît, cette diminution s'est produite à un moment où de nombreuses organisations sont passées au télétravail en raison de la pandémie. Compte tenu des risques d'atteinte à la vie privée que présentent le télétravail et les modalités de travail hybrides, nous nous serions plutôt attendus à une augmentation du nombre de déclarations reçues.

Dans le but de continuer à réaliser des gains d'efficacité, d'offrir une plus grande certitude aux entreprises et de fournir un service de haute qualité aux Canadiens, nous avons eu recours à

divers outils au cours de la dernière année pour fermer les dossiers d'enquête aussi efficacement que possible, de sorte que nous avons fermé uniquement par règlement rapide plus de 85 % des dossiers sous le régime de la LPRPDE.

Un recours accru au processus de règlement rapide et d'autres gains d'efficacité se sont traduits par une réduction considérable du délai de traitement des enquêtes sur les plaintes, qui est passé à 7,8 mois, alors qu'il était de 12,2 mois au cours du dernier exercice.

Comme nous l'avons déjà mentionné, notre arriéré de dossiers a commencé à augmenter cette année, après l'expiration du financement temporaire obtenu dans le cadre du budget fédéral de 2019. À la fin de mars 2021, il restait 29 plaintes sous le régime de la LPRPDE qui remontaient à plus de 12 mois, ce qui représente environ 12 % de nos enquêtes actives relevant de cette loi. Nous nous efforcerons de cerner d'autres possibilités de gains d'efficacité afin d'éviter de nous retrouver avec un arriéré important.

La section qui suit présente certains résultats clés obtenus par le Commissariat en 2021-2022 sous le régime de la LPRPDE.

Atteintes au titre de la *Loi sur la protection des renseignements personnels et les documents électroniques*

L'an dernier, nous avons reçu 645 déclarations d'atteinte touchant au moins 1,9 million de comptes canadiens. Le nombre de déclarations a diminué de 17,5 % par rapport à l'exercice précédent. Malgré cette forte diminution, les atteintes demeurent un important sujet de préoccupation pour le Commissariat.

Bien entendu, le Commissariat ne peut faire état que des atteintes dont il a pris connaissance. Compte tenu de l'énorme quantité de renseignements personnels recueillis, utilisés et communiqués sur le marché numérique, il y a lieu de croire que de nombreux cas ne sont pas déclarés ni même détectés.

La diminution du nombre de déclarations est survenue à un moment où les entreprises étaient plus nombreuses à exercer leurs activités en ligne en raison de la pandémie de COVID-19. Dans ce contexte, nous nous serions attendus à observer une augmentation du nombre d'atteintes déclarées par des secteurs comme celui du commerce de détail. Or, les déclarations venant de ce secteur diminuent en fait d'année en année.

Cinq principaux secteurs selon le pourcentage du nombre total d'atteintes déclarées

Secteur de l'industrie	2018-2019	2019-2020	2020-2021	2021-2022
Finances	22 %	19 %	22 %	20 %
Télécommunications	17 %	17 %	14 %	14 %
Assurances	8 %	11 %	9 %	14 %
Services professionnels	4 %	4 %	8 %	12 %
Vente et commerce de détail	18 %	14 %	10 %	8 %
Secteur manufacturier	4 %	3 %	6 %	8 %

Cela dit, la sous-déclaration par les petites et moyennes entreprises continue de nous préoccuper, étant donné qu'elles représentent près de 90 % des entreprises au pays. Dans l'économie numérique actuelle, les petites organisations peuvent souvent recueillir de grandes quantités de renseignements personnels sensibles. La majorité des atteintes à la vie privée déclarées au Commissariat continuent de provenir de grandes organisations.

Pourcentage des atteintes déclarées selon le type

Type d'atteinte	2018-2019	2019-2020	2020-2021	2021-2022
Accès non autorisé	57 %	59 %	64 %	65 %
Communication non autorisée	26 %	21 %	28 %	25 %
Vol	9 %	9 %	5 %	3 %
Perte	9 %	11 %	3 %*	7 %*

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre à 100.

À hauteur de 65 % (419 incidents), les accès non autorisés constituent la principale cause des atteintes déclarées. Ces incidents impliquent souvent des acteurs externes qui ont eu accès à des systèmes. Il est aussi question de cas où des employés ont consulté des renseignements sans autorisation et les ont utilisés à des fins inappropriées.

Parmi les déclarations mettant en cause un accès non autorisé, 290 (69 %) étaient attribuables à divers types de cybermenaces – maliciels, rançongiciels, piratage et hameçonnage.

Nous avons aussi constaté que le quart des atteintes étaient causées par des communications non autorisées, entre autres, en raison d'erreurs commises par des employés, telles que des communications mal acheminées, ou des communications découlant d'une défaillance des mesures de protection techniques et des vulnérabilités des systèmes.

Amélioration de l'efficacité de nos processus de gestion des atteintes

Le Commissariat s'est efforcé de mettre en œuvre plusieurs mesures pour simplifier ses processus de déclaration et d'examen des atteintes afin qu'il puisse donner plus rapidement une rétroaction aux organisations.

Au cours de l'exercice 2019-2020, le Commissariat a lancé un portail sécurisé pour la déclaration des atteintes, qui permet aux entreprises de soumettre facilement leurs rapports d'atteintes et de recevoir instantanément un numéro de dossier pour faciliter les communications au sujet de la déclaration.

Comme nous l'avons déjà mentionné, les organisations assujetties à la LPRPDE sont tenues de déclarer au Commissariat toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels qui présentent un risque réel de préjudice grave (RRPG) pour les intéressés.

Afin de nous aider à évaluer la conformité aux exigences de déclaration obligatoire, nous avons mis au point un nouvel outil novateur, fondé sur la science du risque, pour évaluer les préjudices liés aux atteintes. Cet outil prend en compte des facteurs comme le degré de sensibilité des renseignements personnels en cause et la probabilité que ces renseignements aient été ou soient mal utilisés ou encore qu'ils soient sur le point de l'être. Nous nous servons déjà de cet outil à l'interne, mais nous prévoyons lancer une version pour le public d'ici la fin de 2022. Le but est, d'une part, de cerner plus rapidement et systématiquement les atteintes qui présentent un risque réel de préjudice grave – à déclaration obligatoire – et, d'autre part, de donner une orientation aux organisations assujetties à la LPRPDE qui déclarent des atteintes afin de les aider à mieux évaluer les risques, gérer les incidents et atténuer les préjudices subis par les Canadiens visés.

Réforme législative et déclaration des atteintes

Compte tenu des retombées positives sur la protection de la vie privée des Canadiens, nous sommes d'avis que toute loi future sur la protection des renseignements personnels dans le secteur privé devrait continuer d'imposer la déclaration obligatoire des atteintes aux mesures de sécurité qui ont trait à des renseignements personnels présentant un risque réel de préjudice grave pour les intéressés. Cependant, en raison du délai observé avant la déclaration des atteintes au Commissariat, nous avons recommandé aux organisations tenues de déclarer une

atteinte de le faire au plus tard sept jours après en avoir pris connaissance. Même si le projet de loi C-27 maintient les obligations des organisations en ce qui a trait à la déclaration des atteintes à la vie privée, il conserve les dispositions actuelles de la LPRPDE selon lesquelles la déclaration des atteintes doit être faite au Commissariat « le plus tôt possible après que l'organisation a conclu qu'il y a eu une atteinte ».

Enquêtes sur les atteintes

MGM Resorts en cause dans une atteinte à la vie privée qui a touché 1,9 million de Canadiens

En 2020, le Commissariat a communiqué avec MGM Resorts International Inc. après avoir appris dans les médias qu'une atteinte à la sécurité des données survenue sept mois plus tôt visait plus de 10 millions de personnes. N'ayant pas reçu de déclaration d'atteinte à la vie privée au sujet de cet incident, le Commissariat a voulu en savoir plus. Il tenait notamment à savoir si les renseignements personnels de Canadiens étaient visés.

Après avoir été contactée par le Commissariat en février 2020, MGM a analysé l'atteinte en question et confirmé que près de deux millions de Canadiens avaient été visés, y compris 5 635 personnes dont les identifiants de documents délivrés par le gouvernement (p. ex. numéro de passeport, numéro de carte NEXUS, numéro de carte d'assurance-maladie ou numéro de carte d'identité militaire) avaient été compromis. En juin 2020, MGM a déclaré cette atteinte au Commissariat et a commencé à aviser les Canadiens visés.

Vu les répercussions éventuelles de l'atteinte et le délai considérable entre le moment où MGM a confirmé l'atteinte et celui où elle a évalué ses répercussions pour les Canadiens, une plainte a été déposée à l'initiative du commissaire pour ouvrir une enquête. Le but de cette enquête était d'établir si l'entreprise avait bien respecté ses obligations en matière de déclaration obligatoire en vertu de la LPRPDE. Plus précisément, nous avons analysé si l'atteinte, selon le critère de déclaration établi dans la *Loi*, présentait un risque réel de préjudice grave et, le cas échéant, si MGM avait avisé le Commissariat le plus tôt possible, comme le prévoit la LPRPDE.

Faisant valoir « l'état médiocre et désorganisé des données, la possibilité que les renseignements en cause soient expirés ou non valides et la nature non sensible des données contenues dans les dossiers visés », MGM a conclu à l'issue de son évaluation des risques que l'atteinte n'exposait pas les personnes visées à un risque réel de préjudice grave.

Le Commissariat estime que les identifiants de documents délivrés par le gouvernement constituent des renseignements sensibles, à l'instar des autres données visées par l'atteinte, lorsqu'ils sont combinés à d'autres renseignements personnels. D'après notre analyse technique, nous avons constaté qu'un acteur malveillant pourrait, en peu de temps et sans trop d'effort, organiser les données d'une façon permettant de déterminer les renseignements personnels visés par l'atteinte.

Nous avons donc constaté que l'atteinte constituait un risque réel de préjudice grave pour les personnes visées, que MGM a attendu sept mois avant d'amorcer son analyse des risques (car elle a d'abord concentré ses efforts sur les clients américains visés, qui ont été avisés de l'atteinte en septembre 2019, c'est-à-dire deux mois après les faits), et que l'entreprise n'avait pas avisé le plus tôt possible le Commissariat ni les personnes visées.

MGM a commencé à aviser les Canadiens visés en juin 2020, soit près de 11 mois après avoir pris connaissance de l'atteinte. En raison de ce délai, les Canadiens concernés n'ont pas pu, pendant près d'un an, prendre de mesures pour atténuer tout autre préjudice susceptible de découler de cette atteinte à leurs renseignements personnels.

MGM s'est engagée à modifier son cadre d'intervention en cas d'atteinte à la vie privée. Ainsi, lorsque l'entreprise prendra connaissance d'une atteinte pouvant toucher des résidents canadiens, elle pourra :

- établir rapidement s'il y a un risque réel de préjudice grave, conformément au document d'orientation publié par le Commissariat;
- faire une déclaration au Commissariat et aviser les personnes visées le plus tôt possible, le cas échéant.

Le Commissariat a donc conclu que la plainte était fondée et qu'elle avait été conditionnellement résolue.

Pour en savoir davantage

- Une enquête sur une atteinte visant MGM illustre comment évaluer le risque et la nécessité d'une évaluation en temps opportun

Une chaîne d'hôtels découvre une atteinte à la sécurité d'une base de données sur la clientèle après l'acquisition d'un concurrent

Marriott International, Inc. a été victime d'une atteinte à la sécurité des données attribuable à l'accès non autorisé à une base de données des hôtels Starwood dont elle a fait l'acquisition en 2016. Marriott a fait savoir qu'un pirate informatique avait accédé à des renseignements personnels contenus dans environ 339 millions de dossiers, dont quelque 12,8 millions où le Canada était indiqué comme pays de résidence.

Cette atteinte visait le profil et les coordonnées des clients participant au programme de fidélité Starwood Preferred Guest ainsi que les renseignements sur leur compte et leurs réservations. Dans le cas de certaines personnes, le pirate avait aussi eu accès aux renseignements figurant sur leur passeport (numéro, code de pays ou pays de délivrance) ou aux renseignements chiffrés relatifs à leur carte de paiement.

En réponse à l'atteinte, Marriott a retenu les services d'un cabinet d'avocats externe et d'une firme tierce d'experts judiciaires. Elle a aussi déployé des outils de surveillance et d'investigation informatique améliorés sur le réseau de Starwood et installé des outils de surveillance supplémentaires dans les centres de données de Starwood pour signaler tout comportement suspect. Marriott a aussi commencé à aviser les personnes visées, et elle a mis à jour son plan de sécurité.

Au cours de notre enquête, nous avons appris que le pirate avait introduit des maliciels dans le système de Starwood avant que Marriott fasse l'acquisition de ce système. Nous avons aussi appris que certaines allégations formulées dans les plaintes étaient fondées, car les mesures de protection et de responsabilité de Marriott étaient inadéquates au moment de l'atteinte. Ces lacunes mettent en évidence les leçons essentielles que toutes les organisations doivent retenir

afin d'éviter ou d'atténuer les dommages occasionnés par une atteinte à la vie privée. Entre autres, il est important que les organisations prennent les mesures suivantes :

- continuer de tester les logiciels antivirus et les contrôles d'accès en cernant et en corrigeant rapidement les lacunes dans ces mesures de protection;
- avoir recours à des méthodes de chiffrement appropriées pour protéger les renseignements personnels;
- détruire les renseignements personnels en temps opportun selon des processus adéquats;
- cerner les menaces en établissant et en mettant en œuvre un système complet de journalisation et de surveillance;
- évaluer et examiner en continu les mesures de sécurité, ce qui est particulièrement important lorsque les organisations acquièrent de nouveaux actifs (comme Marriott l'a fait dans le présent cas).

Depuis l'atteinte, Marriott a apporté un certain nombre d'améliorations. Par exemple, en plus de soumettre régulièrement les serveurs de l'entreprise à des analyses de vulnérabilité, elle a amélioré le processus d'authentification autorisant l'accès des employés à certains comptes (notamment les systèmes des ressources humaines et de la paie). Elle a aussi mis à jour ses politiques de gestion des incidents et des crises.

De plus, Marriott a accepté de retenir les services d'un évaluateur externe chevronné et accrédité pour évaluer en toute indépendance les améliorations qu'elle a apportées, afin d'éviter qu'une atteinte à la vie privée semblable ne se reproduise dans ses systèmes.

Le Commissariat a donc conclu que la plainte était fondée et qu'elle avait été conditionnellement résolue.

Pour en savoir davantage

- Après l'acquisition d'une entreprise concurrente, une chaîne hôtelière découvre une atteinte à sa base de données de clients

Application de la *Loi sur la protection des renseignements personnels et les documents électroniques*

Statistiques et tendances générales concernant les plaintes et les enquêtes

En 2021-2022, le Commissariat a accepté 427 plaintes déposées en vertu de la LPRPDE, ce qui représente une hausse de 38 % par rapport aux 309 plaintes acceptées au cours de l'exercice précédent.

La plupart des plaintes ont été déposées contre des entreprises des secteurs des finances (24 %), des télécommunications (12 %), d'Internet (10 %) et de l'hébergement (10 %). Les plaintes déposées par les individus portaient en grande partie sur l'utilisation et la communication de renseignements personnels (36 %). Viennent ensuite l'accès (28 %), la collecte (13 %) et la conservation (8 %) de renseignements personnels.

Comme nous l'avons déjà souligné, notre formulaire de plainte en ligne continue de nous aider à réaliser des gains d'efficacité. Il nous permet de mieux diriger les plaignants et de demander dès le début du processus les documents et les renseignements nécessaires, ce qui réduit les échanges avec ceux-ci et avec les intimés.

Le Commissariat a fermé 358 plaintes en 2021-2022, ce qui représente une augmentation de 21 % par rapport aux 296 plaintes fermées en 2020-2021.

Enquêtes

Tim Hortons a enfreint les lois sur la protection des renseignements personnels en recueillant de grandes quantités de données personnelles au moyen de son application

L'enquête conjointe que le Commissariat a menée avec ses homologues du Québec, de l'Alberta et de la Colombie-Britannique a révélé que l'application mobile de Tim Hortons suivait et enregistrait les déplacements des clients à quelques minutes d'intervalle, chaque jour, même lorsque l'application n'était pas ouverte. L'entreprise a utilisé ces renseignements pour déduire l'emplacement du lieu de résidence et du lieu de travail des utilisateurs et quand ils voyageaient ou se rendaient chez un concurrent.

Nous avons conclu que cette vaste et continuelle collecte d'une grande quantité de données de géolocalisation par Tim Hortons n'était pas proportionnelle aux avantages que l'entreprise aurait pu espérer tirer d'une publicité ciblée améliorée faisant la promotion de son café et de ses autres produits. Par conséquent, cette pratique était « inappropriée » et constituait une infraction aux lois canadiennes sur la protection des renseignements personnels.

En outre, l'enquête a révélé que Tim Hortons avait tenté d'obtenir un consentement en ayant recours à des déclarations nébuleuses et, dans certaines circonstances, trompeuses qui ne permettaient pas aux utilisateurs de comprendre les conséquences d'un consentement au suivi par l'application.

Tim Hortons a cessé d'effectuer le suivi continuel des données de géolocalisation des utilisateurs en 2020, après le début de l'enquête. Cependant, cette décision n'a pas éliminé le risque de surveillance. L'enquête a révélé que le contrat qu'avait conclu Tim Hortons avec un

tiers américain fournisseur de services de géolocalisation contenait un libellé à ce point large et peu encadré que ce tiers aurait pu vendre les données de géolocalisation « dépersonnalisées » (mais susceptibles d'être réidentifiées) à ses propres fins.

L'enquête a également permis de démontrer que Tim Hortons n'avait pas établi, pour l'application, un programme rigoureux de gestion de la protection de la vie privée, ce qui lui aurait permis de cerner et de prévenir de manière proactive un grand nombre, voire la totalité, des atteintes révélées par l'enquête.

Les quatre autorités de protection de la vie privée ont formulé un certain nombre de recommandations. Elles ont notamment recommandé à Tim Hortons de supprimer toutes les données de géolocalisation restantes et d'exiger des fournisseurs de services tiers qu'ils fassent de même.

Tim Hortons a accepté de mettre en œuvre ces recommandations. Le Commissariat a donc conclu que la plainte était fondée et qu'elle avait été conditionnellement résolue.

Pour en savoir davantage

- Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons (1er juin 2022)

Une entreprise de télécommunications a omis d'obtenir un consentement approprié pour l'inscription à un programme d'authentification faisant appel à l'empreinte vocale

Dans une plainte déposée contre Rogers, une cliente a affirmé que l'entreprise l'avait inscrite à son programme d'authentification biométrique, Empreinte vocale, malgré son refus d'y participer. Après avoir découvert que Rogers l'avait inscrite, la plaignante a appelé l'entreprise pour se retirer encore une fois du programme. Au cours d'un appel ultérieur, elle a découvert que Rogers l'avait de nouveau inscrite à son insu et sans son consentement.

Rogers a dit aux enquêteurs que le programme Empreinte vocale était une solution d'authentification et de lutte contre la fraude conçue pour protéger les comptes des clients. Ce programme utilise des empreintes vocales basées sur des algorithmes, qui sont créées lorsque des personnes communiquent avec les centres d'appels. Quand la personne rappelle, le programme peut établir une correspondance avec son empreinte vocale afin d'authentifier l'identité de l'appelant.

Au terme d'une enquête, nous avons conclu que Rogers avait omis d'obtenir un consentement valable pour l'inscription à son programme Empreinte vocale.

Vu la sensibilité des empreintes vocales biométriques, nous avons conclu qu'un consentement explicite est requis avant la collecte. Or, Rogers a recueilli les empreintes vocales dans le cadre des appels avant de demander un consentement.

Rogers exigeait apparemment que ses agents du service à la clientèle obtiennent un consentement explicite avant d'associer l'empreinte vocale à un compte. Nous avons toutefois constaté que ces agents avaient omis d'obtenir un consentement explicite de la plaignante en l'espèce.

Nous avons également constaté que les agents du service à la clientèle pouvaient facilement contourner l'exigence relative à l'obtention du consentement et que les processus, la formation et la surveillance visant à assurer le respect, par les agents, des protocoles de Rogers en matière de consentement comportaient des lacunes. Pour ces raisons, nous avons conclu que l'entreprise n'avait pas obtenu un consentement valable pour l'inscription à son programme Empreinte vocale.

Nous avons aussi constaté que Rogers avait conservé à tort, sans aucun motif valable, les empreintes vocales des personnes qui s'étaient retirées du programme. L'entreprise avait l'intention de continuer d'utiliser les empreintes vocales pour détecter les fraudes, mais elle ne l'a jamais fait.

En réponse à notre enquête, Rogers a accepté d'apporter un certain nombre de modifications importantes à son programme Empreinte vocale. L'entreprise s'est engagée à obtenir le consentement explicite des clients, à informer ces derniers plus clairement qu'ils ont la possibilité de se désinscrire du programme et, le cas échéant, à supprimer leur empreinte vocale. De plus, Rogers supprimera l'empreinte vocale des personnes qui se sont déjà retirées du programme. Elle apportera des changements importants à ses documents de procédure et de formation des agents qui portent sur l'initiative et procédera à une surveillance pour s'assurer que les agents respectent les protocoles en matière de consentement pour le programme Empreinte vocale. Enfin, lorsque les clients déjà inscrits au programme communiqueront avec les centres d'appels, Rogers reconfirmera leur consentement. Le Commissariat a donc conclu que la plainte était fondée et qu'elle avait été conditionnellement résolue.

Pour en savoir davantage

- Une entreprise de télécommunications a omis d'obtenir un consentement approprié pour l'inscription à un programme d'authentification faisant appel à l'empreinte vocale

Une entreprise de services de transport utilise une caméra dotée de la fonction audio dans les cabines de ses camions pour surveiller les chauffeurs

Un camionneur a déposé une plainte au Commissariat au motif que son employeur, Trimac Transportation Services Inc., avait installé dans son véhicule une caméra-témoin de circulation aux fins d'enregistrement audio et vidéo en continu sans son consentement. Le plaignant était particulièrement préoccupé par l'enregistrement audio.

Trimac, l'une des plus grandes entreprises de services de transport en Amérique du Nord, a expliqué qu'elle avait déployé ce système de caméra dans la cabine de ses camions en 2017 afin de protéger ses actifs et d'assurer une utilisation sécuritaire de ses véhicules. Ce système, qui consiste en un petit appareil installé sur la face intérieure du pare-brise, capte des images vidéo orientées vers l'avant et fait des enregistrements audio dans la cabine des camions de Trimac. Si le camionneur adopte l'un des comportements jugés risqués qui figurent sur une liste prédéterminée, le système enregistre des images vidéo, qu'une tierce partie responsable du traitement examine et classe avant de les transférer à Trimac. Au moment du dépôt de la plainte, le système était activé en permanence lorsque le camion était en marche (même au ralenti), même lorsque le camionneur n'était pas en service et qu'il ne conduisait pas.

Nous avons constaté que les camionneurs faisaient l'objet d'une surveillance constante (pouvant aller jusqu'à 24 heures sur 24, 7 jours sur 7), car le système devait être constamment activé pour capter les extraits (audio et vidéo). Nous avons aussi constaté que les extraits transférés à Trimac étaient accessibles à un plus grand nombre d'employés de Trimac que ce qui était nécessaire, et ce, en raison des mesures de protection limitées contre un accès non autorisé.

Nous comprenons l'importance de la sécurité routière et reconnaissons que le système mis en place pouvait être efficace pour encourager des comportements de conduite sécuritaires. Notre enquête a toutefois révélé que l'enregistrement en continu, en particulier lorsque les camionneurs n'étaient pas en service et qu'ils ne conduisaient pas, n'était pas nécessaire pour permettre à Trimac d'atteindre ses objectifs et que l'atteinte à la vie privée résultant de la mise en œuvre du système n'était pas proportionnelle aux avantages que l'entreprise espérait en retirer.

Le Commissariat a recommandé à l'entreprise d'adopter une approche portant moins atteinte à la vie privée, au minimum en veillant à ce que la fonction audio soit activée uniquement lorsque le camionneur est en service, ou qu'il conduit, et à ce que l'accès aux extraits transférés à Trimac soit limité aux personnes qui ont besoin de savoir. L'entreprise a accepté cette recommandation. Le Commissariat a donc conclu que la plainte était fondée et qu'elle avait été conditionnellement résolue.

Pour en savoir davantage

- Enquête sur l'utilisation par Trimac d'un appareil de surveillance vidéo et audio dans les cabines de ses camions

Une entreprise de services de transport exerce une surveillance constante plus intrusive que nécessaire sur ses camionneurs

Dans une affaire similaire, un camionneur a déposé une plainte au motif que son employeur, Oculus Transport Ltd., une entreprise de camionnage interprovinciale, recueillait des enregistrements audio de toutes les conversations qui étaient tenues dans la cabine de son camion, même lorsqu'il n'était pas en service.

Oculus a installé des dispositifs de surveillance dans les cabines de ses camions, principalement pour faciliter les enquêtes en cas d'incident et assurer la conformité aux règlements provinciaux et aux exigences imposées sur les routes privées. Ces dispositifs enregistraient le son à l'intérieur de la cabine et captait des images à travers la fenêtre avant du camion, en plus de fournir des renseignements en temps réel sur l'endroit où se trouvait le camion d'Oculus.

Les enregistrements audio recueillis étaient susceptibles de renfermer des renseignements sensibles, car il pouvait s'agir de conversations tenues par les employés à l'intérieur de la cabine de leur camion, par exemple des conversations privées avec des amis, des parents, des docteurs ou des tierces parties.

Oculus a expliqué que les enregistrements audio étaient protégés contre tout accès non autorisé et qu'il était seulement possible d'y accéder dans des circonstances précises et limitées.

Nous avons accepté l'argument selon lequel la surveillance audio en question visait uniquement à répondre à un besoin légitime et qu'elle pouvait être efficace pour permettre à l'entreprise de réaliser les fins visées. Nous avons toutefois estimé qu'une collecte constante (24 heures sur 24), y compris lorsque les camionneurs n'étaient pas en service ou dormaient dans la cabine de leur camion, portait atteinte à leur vie privée plus que ce qui était nécessaire et que les répercussions sur leur vie privée n'étaient pas proportionnelles aux avantages que la surveillance pouvait procurer à l'entreprise.

Oculus a confirmé au Commissariat qu'elle avait abandonné la surveillance audio. Le Commissariat a donc conclu que la plainte était fondée et qu'elle avait été résolue. Si l'entreprise décidait dans l'avenir d'avoir recours à une surveillance audio dans la cabine, nous nous attendrions à ce qu'elle limite les enregistrements audio à ce qui est nécessaire pour réaliser les fins visées.

Pour en savoir davantage

- Une entreprise de services de transport exerce une surveillance constante plus intrusive que nécessaire sur ses camionneurs

Règlement rapide

Comme en témoigne son utilisation dans la législation applicable au secteur public, le processus de règlement rapide demeure un précieux outil pour traiter en peu de temps les plaintes de nature non systémique. En règle générale, les plaignants obtiennent un résultat en quelques mois, alors que le délai est beaucoup plus long pour d'autres types d'enquêtes. Nous sommes heureux que de nombreuses organisations collaborent avec le Commissariat pour traiter les dossiers dès le début, à la satisfaction mutuelle de toutes les parties concernées, sans qu'il soit nécessaire de mener une enquête approfondie.

En 2021-2022, nous avons fermé par règlement rapide 85 % des plaintes déposées en vertu de la LPRPDE (ce qui représente 303 plaintes), soit la plus forte proportion jamais enregistrée.

Pourcentage des plaintes fermées par règlement rapide

Exercice	Pourcentage des plaintes fermées par règlement rapide
2021-2022	85 %
2020-2021	71 %
2019-2020	69 %
2018-2019	63 %
2017-2018	66 %

En plus de maximiser le recours au règlement rapide, nous continuons de mener des enquêtes sommaires pour résoudre les plaintes, principalement dans les dossiers où il est facile de vérifier les faits, mais où il est impossible de parvenir à un règlement consensuel.

En 2021-2022, l'équipe du règlement rapide au Commissariat a commencé à envoyer des lettres d'avis. Ce nouvel outil simplifie encore davantage le traitement des plaintes les plus courantes et permet ainsi au Commissariat de les résoudre plus rapidement. Ces lettres fournissent des précisions au sujet de la plainte et rappellent aux organisations les obligations qui leur incombent en vertu de la LPRPDE ainsi que les attentes du Commissariat, sans qu'il soit nécessaire de parvenir à une conclusion. Avec le temps, l'utilisation de ce nouvel outil devrait renforcer la capacité du Commissariat à offrir un service rapide aux Canadiens.

Exemples de réussite : processus de règlement rapide

Une entreprise de dépistage de la COVID-19 cesse l'envoi de courriels promotionnels

Une entreprise autorisée par le gouvernement fédéral à administrer les tests obligatoires de dépistage de la COVID-19 à l'Aéroport Montréal-Trudeau a fait l'objet d'une plainte après qu'un voyageur contraint de se soumettre à un test de dépistage a reçu de cette entreprise, sans y avoir consenti, un courriel faisant la promotion de ses autres services.

Au cours de l'enquête ouverte par le Commissariat, Biron Groupe Santé Inc. a indiqué qu'elle considérait, initialement, qu'une relation d'affaires était créée avec les voyageurs concernés et qu'elle pouvait donc présumer du consentement implicite de ces derniers pour leur envoyer des courriels promotionnels.

Après avoir reçu directement plusieurs plaintes de voyageurs et eu des discussions plus approfondies avec le Commissariat, l'entreprise a cessé d'envoyer des courriels promotionnels et supprimé de sa base de données de marketing les adresses courriel de plus de 147 000 voyageurs qui n'étaient pas déjà ses clients.

Le Commissariat a jugé que l'affaire avait été réglée en cours d'enquête et il n'a émis aucune conclusion.

Le Commissariat et la Commission d'accès à l'information du Québec ont collaboré au cours de l'enquête en partageant de l'information utile pour l'examen de la plainte par le Commissariat.

Mise à jour de procédures d'authentification par des entreprises offrant des comptes en ligne

Plusieurs personnes ont déposé une plainte au Commissariat au sujet des exigences en matière d'authentification imposées pour réactiver un compte bloqué sur différentes plateformes en ligne. Les organisations exigeaient une copie d'une pièce d'identité avec photo, par exemple un permis de conduire, pour valider l'identité des titulaires de compte.

Au cours de nos discussions, nous avons appris que le personnel de première ligne qui recevait les demandes de réactivation de compte des plaignants n'indiquait pas à ceux-ci qu'ils pouvaient caviarder certains renseignements figurant sur leur pièce d'identité jugés non nécessaires pour la procédure d'authentification.

En fin de compte, nous avons facilité l'adoption d'une stratégie de communication améliorée pour les entreprises intimées, et les plaignants se sont sentis plus à l'aise avec le processus de récupération de compte. La plainte a donc été fermée par règlement rapide.

Activités de l’unité de vérification de la conformité

Lorsque les organisations signent une entente de conformité, elles acceptent de prendre des mesures contraignantes pour s’assurer que leurs pratiques sont conformes à la loi. Dans d’autres cas, les organisations acceptent de mettre en œuvre nos recommandations au terme d’une enquête.

Lorsqu’une entente de conformité est conclue, il est important que le Commissariat en assure le suivi pour vérifier si les engagements pris sont respectés selon les échéances prévues. Cette tâche incombe à notre unité de vérification de la conformité.

Desjardins est en train de régler les problèmes qui ont donné lieu à la fuite massive de données

En mai 2019, Desjardins a avisé le Commissariat d’une atteinte à la sécurité des données qui a finalement touché près de 9,7 millions d’individus au Canada et à l’étranger. Il s’agit de la plus importante atteinte à la sécurité des données survenue à ce jour dans le secteur des services financiers canadiens. Nous avons constaté que des lacunes administratives et technologiques avaient permis à un employé de Desjardins de consulter et d’extraire les renseignements personnels de clients (nom, date de naissance, numéro d’assurance sociale, adresse résidentielle, adresse courriel et historique des transactions).

À l’issue de notre enquête, menée en collaboration avec la Commission d’accès à l’information du Québec, nous avons conclu que Desjardins avait contrevenu à la LPRPDE en ce qui concerne les principes de responsabilité, de la conservation et des mesures de sécurité.

Desjardins a accepté de mettre en œuvre nos recommandations visant à mettre à niveau son programme de sécurité de l’information et de protection des renseignements personnels, y compris ses pratiques de destruction des données. L’institution financière s’est également engagée à retenir les services de vérificateurs externes pour évaluer et attester ce programme et à présenter un rapport d’évaluation au Commissariat.

Desjardins se montre coopérative. Tous les six mois, elle présente au Commissariat des rapports d’étapes sur l’exécution d’un plan d’action exhaustif visant à résoudre les problèmes en question. La mise en œuvre de nos recommandations et de son plan d’action va bon train. En décembre 2022, l’institution doit présenter au Commissariat un rapport d’audit de ses mesures visant à améliorer la gouvernance, la reddition de comptes et la sécurité.

Le Commissariat continuera de surveiller les progrès réalisés par l’institution financière jusqu’à ce que celle-ci ait fait la preuve de la mise en œuvre des recommandations formulées dans le rapport de conclusions final.

Pour en savoir davantage

- Enquête sur la conformité à la LPRPDE de Desjardins suite à l’atteinte aux mesures de sécurité des renseignements personnels entre 2017 et 2019 (14 décembre 2020)
- Un ensemble de lacunes a donné lieu à la fuite massive de données chez Desjardins (14 décembre 2020)

Conseils et activités de sensibilisation à l’intention des entreprises

La Direction des services-conseils à l’entreprise aide les entreprises assujetties à la LPRPDE à évaluer et à gérer de façon proactive les risques d’atteinte à la vie privée que présentent leurs initiatives et leurs pratiques. L’objectif de cette direction est d’aider ces entreprises à se conformer à la *Loi* lorsqu’elles adoptent de nouvelles technologies et des modèles d’affaires novateurs.

Le Commissariat a mené toute une série d’activités de promotion de la conformité pour fournir aux entreprises des conseils précis et pratiques afin de bien les renseigner et de les orienter quant aux obligations qui leur incombent en vertu de la LPRPDE. En 2021-2022, nous avons en tout lancé 14 nouvelles activités dans le domaine des services-conseils et mené 25 activités de sensibilisation dans divers secteurs industriels. Dix-huit consultations étaient en cours à la fin de l’exercice.

Les exemples présentés ci-dessous illustrent le travail accompli par la Direction des services-conseils à l’entreprise.

Apple poursuit la consultation au sujet du projet de récupération des images pour Apple Maps

De son propre chef, Apple a eu recours aux services-conseils du Commissariat pour la première fois en 2019 concernant son projet de récupération des images pour Apple Maps au Canada. La Direction des services-conseils à l’entreprise du Commissariat a depuis donné à Apple des conseils en matière de conformité à la LPRPDE et des recommandations sur la protection de la vie privée à diverses étapes successives du projet de représentation cartographique et de cartographie des rues dans l’application Apple Maps. Vu la portée de ce projet, nous avons demandé l’avis de nos homologues provinciaux qui ont des lois sur la protection des renseignements personnels très semblables à la LPRPDE. Les recommandations que nous avons récemment formulées reposent sur des conseils antérieurs en matière de conformité à la LPRPDE. L’entreprise les a bien accueillies.

Une PME sollicite des conseils sur le marché en ligne de talents artistiques

Une PME a communiqué avec le Commissariat après avoir participé à l’une de ses cliniques virtuelles sur la protection de la vie privée afin de demander des services-conseils sur son marché en ligne de talents créatifs. Plus précisément, elle a demandé des conseils exhaustifs sur ses pratiques de gestion des renseignements personnels. La PME a accueilli favorablement les conseils donnés et s’est montrée réceptive aux recommandations formulées.

Programme des contributions

Chaque année, le Commissariat poursuit l'élaboration de politiques en matière de protection de la vie privée et fait la promotion de la protection des renseignements personnels dans le secteur privé grâce à son Programme des contributions. Depuis sa création en 2004, le Programme a alloué environ 8 millions de dollars à près de 180 projets.

Pour le cycle de financement 2022-2023, le Commissariat a sollicité des propositions de projets de recherche sur le thème « Qui est touché et de quelle manière : évaluer et atténuer les risques, les obstacles et les inégalités en matière de protection de la vie privée ». Le Commissariat voulait se pencher sur les expériences, les obstacles et les inégalités dans ce domaine avec lesquels divers groupes de personnes doivent composer ainsi que sur la manière dont il est possible d'en atténuer les répercussions.

Après avoir évalué en fonction de leur mérite les 33 propositions reçues, nous avons sélectionné 11 projets de recherche. Nous avons octroyé jusqu'à 50 000 $ par projet, sur un budget total de 500 000 $, à divers organismes à but non lucratif, notamment des établissements d'enseignement supérieur et des organismes de défense des droits. Les projets retenus cette année porteront sur des sujets comme l'examen des répercussions de l'application de la LPRPDE sur la souveraineté des données des Premières Nations, l'opinion du public sur la technologie de reconnaissance faciale et la vie privée dans les salles de classe virtuelles.

En 2021-2022, le Commissariat a redoublé d'efforts pour attirer un plus large éventail de demandes. Il a donc été ravi de recevoir des propositions de partout au Canada, dont une du Nunavut, qui a été retenue. Le projet proposé portera sur la protection de la vie privée, l'intelligence artificielle et l'apprentissage automatique selon « le point de vue des collectivités rurales, éloignées et autochtones ».

Pour en savoir davantage

- Le Commissariat annonce les nouveaux bénéficiaires de financement pour des projets indépendants de recherche : Évaluer et atténuer les risques, les obstacles et les inégalités en matière de protection de la vie privée (20 juin 2022)
- Projets en cours financés par le Programme des contributions (20 juin 2022)

Points saillants des autres travaux menés par le Commissariat

Points saillants des autres travaux menés par le Commissariat

Conseils au Parlement

L'exercice 2021-2022 a été une autre année inhabituelle, la COVID-19 et les élections fédérales ayant perturbé les travaux parlementaires courants.

Le Commissariat a continué de collaborer de manière proactive avec le Parlement. Nous avons comparu plusieurs fois devant divers comités parlementaires pour exprimer notre point de vue dans le cadre de l'examen de projets de loi et d'études portant sur des sujets tels que l'utilisation et les impacts de la technologie de reconnaissance faciale, la collecte et l'utilisation de données sur la mobilité par le gouvernement du Canada, ainsi que la limitation de l'accès en ligne des jeunes au matériel sexuellement explicite.

Étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale

Lors de sa comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) au début de mai 2022, le commissaire a exprimé son point de vue sur l'utilisation et les impacts de la technologie de reconnaissance faciale. Le Comité ETHI avait entrepris une étude de ces deux aspects de la nouvelle technologie en question.

Le commissaire a alors souligné les travaux du Commissariat dans le domaine, notamment nos enquêtes sur les pratiques de Clearview AI et sur l'utilisation de la technologie de cette entreprise par la Gendarmerie royale du Canada, ainsi que notre consultation publique nationale sur le recours à la reconnaissance faciale par les services de police. Cette consultation a donné lieu à une déclaration commune des gardiens de la vie privée fédéral, provinciaux et territoriaux à la protection de la vie privée sur la nécessité d'adopter un cadre législatif qui établirait des mesures de protection contre les risques associés à cette technologie. (On trouvera plus de précisions à ce sujet dans la section consacrée à la réforme législative.)

Pour en savoir davantage

- Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) au sujet de l'étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale (2 mai 2022)

Collecte et utilisation de données sur la mobilité à des fins de traçage de cas de COVID-19

En février, le Commissariat a comparu devant le Comité ETHI dans le cadre de son étude sur la collecte et l'utilisation de données sur la mobilité par le gouvernement du Canada.

Nous avons alors souligné que cette situation montre l'urgence d'une réforme législative – dans ce cas-ci afin d'autoriser l'utilisation des données personnelles pour le bien commun ou à des fins commerciales légitimes, à l'intérieur d'une loi fondée sur les droits qui reconnaîtrait la nature et l'importance du droit à la vie privée en tant que droit de la personne. Nous avons ajouté que la circulation des données entre les secteurs privé et public montre que ces deux secteurs doivent être assujettis à des normes similaires et régis par des règles et des principes communs.

Le Commissariat a reçu des plaintes concernant l'utilisation de ce type de renseignements par l'Agence de santé publique du Canada (ASPC) dans le cadre des activités menées par cet organisme pour suivre la propagation de la COVID-19. Comme une enquête était en cours au moment de notre comparution, nous n'étions pas en mesure d'indiquer si les renseignements avaient été dépersonnalisés adéquatement.

Pour en savoir davantage

- Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) au sujet de l'étude sur la collecte et l'utilisation de données sur la mobilité par le gouvernement du Canada (7 février 2022)
- Déclaration du commissaire à la protection de la vie privée à la suite de la publication du rapport du Comité ETHI sur la collecte et l'utilisation par le gouvernement de données sur la mobilité (4 mai 2022)

Comparution dans le cadre de l'examen d'un projet de loi visant à limiter l'accès en ligne des jeunes au matériel sexuellement explicite

Le commissaire a comparu devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles dans le cadre de l'examen du projet de loi S-203, *Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite*. Il a alors souligné que le Commissariat soutenait les efforts visant à accorder une attention particulière aux droits des enfants dans l'environnement numérique, mais que le projet de loi soulevait plusieurs enjeux sur le plan de la protection de la vie privée en raison de l'obligation de recueillir des renseignements personnels pour faciliter la vérification de l'âge.

Pour en savoir davantage

- Comparution devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles concernant le projet de loi S-203, *Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite* (2 juin 2021)

Présentation d'un mémoire dans le cadre d'une consultation menée par un sénateur au sujet de la *Loi sur la concurrence*

Le Commissariat a été invité à participer à la consultation menée par le sénateur Howard Wetston au sujet de la *Loi sur la concurrence* à l'ère numérique. Pour fournir nos observations, nous nous sommes appuyés sur l'expérience de leadership du Commissariat dans ce domaine à titre de coprésident du Groupe de travail sur le citoyen et le consommateur

numérique de l'Assemblée mondiale pour la protection de la vie privée, qui se penche sur des enjeux à l'intersection de la protection de la vie privée et de la législation sur la concurrence.

Dans son mémoire, le Commissariat a fait valoir que la nature de l'économie numérique donne lieu à de plus grandes intersections entre les régimes réglementaires qui encadrent la protection de la vie privée, la concurrence et la protection des consommateurs. Les considérations en matière de vie privée et de données prendront une importance croissante dans la politique de la concurrence, si bien que la collaboration inter-réglementaire deviendra de plus en plus nécessaire.

Pour en savoir davantage

- Examen de la *Loi sur la concurrence* au Canada à l'ère numérique (21 décembre 2021)

Coopération avec des autorités canadiennes et étrangères

La coopération au pays et à l'échelle internationale en matière d'application des lois sur la protection des renseignements personnels, ainsi qu'entre les sphères de réglementation, s'avère de plus en plus essentielle dans un monde numérique où les flux de données transcendent les frontières. La collaboration intergouvernementale et inter-réglementaire permet de mieux protéger les droits des citoyens. La collaboration dans le domaine de l'application des lois accroît notre capacité à prendre des mesures et accentue les retombées de ces mesures sur la conformité. Elle procure également des avantages aux organismes en simplifiant les processus d'enquête et en favorisant une plus grande harmonisation dans l'application des lois.

La coopération avec d'autres autorités de protection des données, au Canada et à l'étranger, est devenue au fil des ans un élément de plus en plus important de notre travail, et la coopération avec des autorités de l'extérieur du domaine de la protection de la vie privée, notamment dans le domaine de la concurrence, commence à prendre de l'ampleur. La section qui suit présente certaines initiatives clés menées en 2021-2022.

Coopération internationale

La protection des renseignements personnels des Canadiens passe de plus en plus par l'application des lois canadiennes à l'encontre d'entreprises qui sont établies et exercent leurs activités dans d'autres pays.

Le Commissariat suit les derniers développements sur la scène internationale dans les domaines juridique, technologique et commercial qui pourraient toucher le Canada. Nous participons à plusieurs tribunes mondiales et régionales, ainsi qu'à des forums linguistiques, où les autorités de protection de la vie privée mettent en commun leur expérience et coordonnent leurs efforts consacrés à l'élaboration de politiques et à l'établissement de pratiques exemplaires. Ces types d'activités offrent des possibilités intéressantes et procurent des avantages de taille lorsqu'il s'agit d'améliorer l'efficacité opérationnelle et l'ensemble des mesures de protection de la vie privée de la population canadienne.

Voici quelques exemples des activités que nous avons menées en 2021-2022 dans le cadre de collaborations internationales.

Assemblée mondiale pour la protection de la vie privée

Le Commissariat est un membre actif de l'Assemblée mondiale pour la protection de la vie privée (AMVP), qui regroupe plus de 130 autorités de protection des données et de la vie privée du monde entier et joue un rôle de premier plan en favorisant la collaboration internationale. Il participe à divers groupes de travail de l'AMVP, dans certains cas à titre de président, et prend part à des travaux concertés portant sur des sujets d'importance mondiale – p. ex. l'intelligence artificielle et la technologie de reconnaissance faciale, l'éducation numérique et le partage de données. De plus, nous parrainons des résolutions sur ces questions et d'autres sujets d'intérêt mondial et participons à la rédaction de ces documents.

Groupe de travail international sur la protection de la vie privée et les droits de la personne

À la présidence de ce groupe de travail de l'AMVP, le Commissariat a supervisé l'adoption d'un rapport sur la protection de la vie privée et la protection des données en tant que droits fondamentaux. Ce rapport examine le lien entre la protection de la vie privée et les autres droits fondamentaux.

Conférence de 2021 et résolutions adoptées

La promotion d'une approche axée sur l'être humain et la mise en place d'un environnement réglementaire mondial ayant des normes élevées en matière de protection des données étaient les principaux thèmes de la 43e conférence de l'AMVP, qui s'est tenue en mode virtuel en octobre 2021. Plusieurs résolutions ont alors été adoptées, dont celles-ci :

- une résolution (en anglais seulement) préconisant le respect des principes fondamentaux de protection de la vie privée lorsque les gouvernements accèdent à des renseignements personnels détenus par l'entreprise privée pour des fins de sécurité nationale et de sécurité publique;
- une résolution sur les droits numériques des enfants visant à renforcer la protection de ces droits;
- une résolution portant sur la mise sur pied d'un groupe de travail de l'AMVP qui se penchera sur les façons dont les données peuvent être échangées pour servir le bien public.

Groupe de travail sur la coopération internationale en matière d'application de la loi

Le Commissariat demeure coprésident du Groupe de travail de l'AMVP sur la coopération internationale en matière d'application de la loi. Vu l'importance fondamentale de la coopération dans ce domaine, il s'agit d'un groupe de travail permanent de l'AMVP. Il a pour mandat de favoriser une coopération proactive et pratique pour l'application de la loi à l'égard de questions essentielles qui présentent un intérêt pour les membres du milieu international de l'application des lois sur la protection des renseignements personnels.

Le groupe de travail en question, qui compte 34 membres, sert de tribune pour la coopération en matière d'application de la loi. Il a tenu plusieurs séances virtuelles pour discuter des risques d'atteinte à la vie privée d'envergure mondiale comme les technologies publicitaires et le ratissage de données. Ces discussions ont conduit à la création de sous-groupes chargés de sujets particuliers afin de faire progresser les initiatives dans le domaine de la conformité. Le Commissariat a contribué à plusieurs de ces sous-groupes, plus précisément les suivants :

- le sous-groupe sur le bourrage d'identifiants, pour élaborer des orientations à l'intention des organisations et du public;
- le sous-groupe sur le ratissage de données, pour rédiger une déclaration commune visant à faire connaître les risques liés à cette pratique et les stratégies d'atténuation connexes;
- le sous-groupe sur les technologies publicitaires, pour mieux comprendre les enjeux liés à l'écosystème de ces technologies;
- le sous-groupe sur la reconnaissance faciale, qui relève du Groupe de travail sur la coopération internationale en matière d'application de la loi et du Groupe de travail sur

l'éthique et la protection des données en matière d'IA, pour établir les principes et les attentes se rapportant à l'utilisation des renseignements personnels dans les technologies de reconnaissance faciale.

Groupe de travail sur le citoyen et le consommateur numérique

Le Commissariat copréside le Groupe de travail sur le citoyen et le consommateur numérique. Depuis 2017, ce groupe se penche sur les recoupements croissants entre la protection de la vie privée, la concurrence et la protection des consommateurs. Il favorise aussi la collaboration dans ces domaines où se recoupent plusieurs régimes réglementaires. Vu l'importance des travaux menés dans le but de garantir une économie numérique mondiale respectueuse de la vie privée, il est récemment devenu un groupe de travail permanent de l'AMVP.

Ce groupe a rédigé un rapport intitulé « La protection de la vie privée et des données en guise de facteurs dans la réglementation de la concurrence : sondage auprès des autorités de réglementation de la concurrence visant à améliorer la collaboration inter-réglementaire », qui a été lancé à l'occasion de la Conférence 2021 de l'AMVP. Le Commissariat est l'auteur principal de ce rapport, qui avait pour objectif de cerner diverses possibilités pour renforcer la collaboration entre les autorités de protection de la vie privée et les organismes de réglementation de la concurrence.

Par ailleurs, le Groupe de travail a commandé un rapport universitaire complémentaire, qui analyse en profondeur les recoupements entre les régimes réglementaires sur la protection de la vie privée et la concurrence, explore les compléments et les tensions entre ces deux sphères réglementaires et expose les avantages de la collaboration inter-réglementaire.

Enfin, le Groupe de travail a fait pression pour que les instruments de réglementation sur la concurrence tiennent davantage compte de la protection de la vie privée. En outre, cette année, il a rédigé un mémoire à la suite de la consultation menée conjointement par la Federal Trade Commission des États-Unis et le département de la Justice des États-Unis visant à moderniser les lignes directrices américaines sur les fusions afin de mieux détecter et prévenir les transactions anticoncurrentielles.

Le Commissariat a joué un rôle de premier plan pour promouvoir et préconiser une coopération inter-réglementaire entre les organismes de réglementation et les principales parties prenantes en prononçant des allocutions publiques et en accordant des entrevues dans les médias. Il continuera d'orienter les discussions mondiales prioritaires à cet égard avec les autorités de protection de la vie privée d'autres administrations.

Pour en savoir davantage

- Rapport annuel du Groupe de travail sur le citoyen et le consommateur numérique (août 2021)

Global Privacy Enforcement Network

Le Global Privacy Enforcement Network (GPEN – réseau mondial d'application des lois sur la protection de la vie privée) permet aux autorités d'application des lois dans ce domaine de mettre en commun leurs connaissances, leur expérience et leurs pratiques exemplaires au chapitre de la coopération et de l'application de ce type de lois. Ce réseau informel assure aussi

la coordination d'initiatives conjointes, comme le ratissage international pour la protection de la vie privée (qui en est maintenant à sa 8e année), afin de favoriser une plus grande conformité aux lois à l'échelle mondiale. Le Commissariat siège au comité de gestion du GPEN avec ses homologues du Royaume-Uni, de Hong Kong, d'Israël et des États-Unis. Le GPEN s'attache à établir des relations solides avec les responsables de l'application de la loi. Il a aussi organisé des ateliers portant sur les enquêtes afin de permettre la mise en commun des stratégies et des techniques.

Le GPEN souligne en 2022 son 10e anniversaire. En février, son comité de gestion a tenu une activité pour amorcer les discussions en vue d'élaborer le nouveau plan d'action du réseau pour la prochaine décennie.

Autorités de protection des données et de la vie privée des pays du G7

En septembre 2021, le Commissariat a participé à une table ronde des autorités de protection des données et de la vie privée des pays du G7. Les discussions ont fait ressortir que ces autorités doivent unir leurs efforts pour élaborer des stratégies permettant de superviser la circulation des données à l'échelle mondiale.

La réunion s'est déroulée dans le contexte de la Feuille de route pour la coopération à l'égard de la libre circulation des données dans la confiance, annoncée en avril 2021 par les ministres chargés du numérique et des technologies des pays du G7.

Cette réunion arrivait à point nommé compte tenu de l'économie mondiale de plus en plus axée sur les données et des changements découlant de la pandémie actuelle.

En tant qu'organismes de réglementation de la protection des données et de la vie privée des économies numériques les plus avancées au monde, les autorités en la matière des pays du G7 ont convenu de renforcer la collaboration, de jouer un rôle de premier plan dans les discussions concernant les enjeux numériques et de contribuer à favoriser l'adoption de normes plus élevées en matière de protection des données à l'échelle mondiale.

Ces autorités ont aussi convenu de se réunir une fois par année pour discuter d'enjeux d'intérêt mutuel. Les membres du groupe pourront ainsi établir une tribune pour des relations, des discussions et une influence à plus long terme réunissant des organisations internationales et d'autres intervenants clés afin de promouvoir les valeurs et les objectifs que les membres ont en commun.

Pour en savoir davantage

- Communiqué publié à l'issue de la Table ronde des autorités de protection des données et de la vie privée des pays du G7 (7 et 8 septembre 2021)

Nouveaux protocoles d'entente

Le Commissariat a renouvelé et mis à jour un protocole d'entente conclu avec l'autorité de protection des données des Pays-Bas (*Autoriteit Persoonsgegevens*) afin de faciliter la communication de renseignements entre les deux organismes.

Il a également signé un protocole d'entente avec le commissaire à la protection des données du Marché international d'Abu Dhabi (Abu Dhabi Global Market) afin de faciliter la communication de renseignements entre les deux organismes.

Collaborations fédérales-provinciales-territoriales

Les commissaires à l'information et à la protection de la vie privée fédéraux, provinciaux et territoriaux se réunissent annuellement pour coordonner leurs activités portant sur les questions de politique publique et de sensibilisation du public. Ils lancent notamment des appels à l'action pour favoriser la mise en place de mesures de protection de la vie privée qui soient uniformes à l'échelle du pays. Leur prochaine réunion annuelle est prévue en septembre 2022 à St. John's (Terre-Neuve-et-Labrador). Les commissaires se réunissent aussi en mode virtuel une fois par mois pour discuter d'enjeux d'intérêt mutuel et faire progresser leurs projets conjoints.

De plus, le Commissariat collabore souvent avec ses homologues provinciaux ou territoriaux dans le cadre d'importantes initiatives. Mentionnons notamment notre appel conjoint aux législateurs pour réclamer un nouveau cadre juridique qui établirait clairement et explicitement les situations où le recours à la reconnaissance faciale par les services de police peut être acceptable, comme nous en avons fait état précédemment dans le présent rapport.

Enfin, fort du succès des enquêtes conjointes sur Clearview AI et Cadillac Fairview menées l'an dernier, le Commissariat a collaboré avec quatre homologues provinciaux dans le cadre d'une enquête importante portant sur l'application mobile de Tim Hortons, comme nous en avons aussi fait état précédemment dans le présent rapport. Le présent exercice représente un moment historique pour la collaboration en matière d'application de la loi à l'échelle nationale, puisque le Commissariat, ainsi que ses homologues de la Colombie-Britannique, de l'Alberta et du Québec, ont reçu le prix pour le règlement des différends de l'AMVP pour leurs mesures de conformité concertées concernant la technologie de reconnaissance faciale.

Protocole d'entente

Le Commissariat a renouvelé un protocole d'entente de longue date conclu avec le Commissariat à l'information et à la protection de la vie privée de l'Alberta et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique pour y intégrer la Commission d'accès à l'information du Québec.

Ce protocole d'entente établit un cadre qui permet de mieux soutenir la collaboration et la coordination à l'échelle fédérale et provinciale de manière à mobiliser les ressources des commissariats pour maximiser la capacité et la répercussion des activités de surveillance, tout en réduisant le dédoublement du travail et le manque d'efficacité. En outre, il contribue à accroître le partage de connaissances et à intensifier les relations entre les commissariats afin de garantir une surveillance uniforme, coordonnée, efficace et harmonisée de la protection des renseignements personnels dans le secteur privé au Canada, et à suivre les instructions communes des commissaires à la protection de la vie privée.

Les principales tribunes pour atteindre les objectifs définis dans ce protocole d'entente sont le Forum sur la protection des renseignements personnels dans le secteur privé et le Forum national de collaboration sur l'application de la loi. Le Forum sur la protection des renseignements personnels dans le secteur privé regroupe des représentants du Commissariat

et d'homologues provinciaux chargés de la surveillance de l'application des lois sur la protection des renseignements personnels dans le secteur privé (Alberta, Colombie-Britannique et Québec). Ses membres se réunissent chaque trimestre pour cerner les possibilités de collaboration dans le domaine de la politique publique et de la sensibilisation du public ainsi que pour se conseiller les uns les autres et se tenir mutuellement informés des initiatives proposées et en cours.

Pour sa part, le Forum national de collaboration sur l'application de la loi facilite les discussions entre les autorités participantes en vue de protéger plus efficacement le droit à la vie privée des Canadiens, notamment en saisissant les occasions de communiquer de l'information et de collaborer à des enquêtes conjointes ou parallèles ainsi qu'en échangeant sur les difficultés que pose l'application de la loi et les solutions pratiques mises au point pour les surmonter.

Par ailleurs, le Commissariat a conclu un protocole d'entente avec le Commissariat à l'information et à la protection de la vie privée du Nunavut afin de faciliter la communication de renseignements entre les deux organismes.

Pour en savoir davantage

- Des gardiens de la vie privée signent une entente de collaboration (10 mai 2022)
- Le CPVP signe une entente d'échange de renseignements avec son homologue du Nunavut (7 décembre 2021)

Devant les tribunaux

Commissaire à la protection de la vie privée du Canada c. Facebook, Inc. (T-190-20) (Cour fédérale) (Facebook 1); Facebook, Inc. c. Commissaire à la protection de la vie privée du Canada (T-473-20) (Cour fédérale) (Facebook 2)

Le litige entre le Commissariat et Facebook s'est poursuivi cette année.

Dans l'affaire Facebook 1, le Commissariat à la protection de la vie privée du Canada a présenté, en février 2020, une demande au titre de l'alinéa 15a) de la LPRPDE en vue d'obtenir une ordonnance, à la suite d'une enquête et la production d'un rapport de conclusions concernant une plainte relative aux pratiques de traitement des renseignements personnels de l'intimée, Facebook, Inc.

L'enquête conjointe menée en 2019 par le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique a révélé de graves lacunes dans les pratiques du géant des médias sociaux en matière de traitement des renseignements personnels. Facebook a contesté les conclusions de l'enquête et refusé de donner suite aux recommandations pour corriger les lacunes relevées.

Le Commissariat à la protection de la vie privée du Canada a alors déposé auprès de la Cour fédérale un avis de demande en vue d'obtenir une déclaration selon laquelle Facebook avait contrevenu à la LPRPDE, ainsi que diverses autres réparations. La Cour fédérale a le pouvoir, entre autres, de rendre des ordonnances exécutoires exigeant qu'une organisation revoie ou modifie ses pratiques et qu'elle se conforme à la loi.

On trouvera dans le Rapport annuel 2018-2019 du Commissariat des précisions à propos de cette enquête et du Rapport de conclusions publié en avril 2019.

Par ailleurs, le Rapport annuel 2019-2020 du Commissariat résume l'avis de demande que nous avons déposé et les réparations qui ont été sollicitées.

En mars 2020, le Commissariat a signifié à Facebook sa preuve par affidavit à l'appui de la demande au titre de l'article 15 de la LPRPDE. Facebook a depuis présenté une motion en radiation de certaines parties de l'affidavit.

En avril 2020, Facebook a également déposé un avis de demande de contrôle judiciaire de notre rapport de conclusions d'enquête en vertu de l'article 18.1 de la *Loi sur les Cours fédérales* (Facebook 2). L'entreprise demande le contrôle judiciaire de notre décision d'enquêter et de continuer d'enquêter ainsi que du processus d'enquête et cherche à faire annuler le rapport de conclusions qui en a résulté.

En réponse, le Commissariat a présenté une requête pour demander la radiation de l'avis de demande de contrôle judiciaire de Facebook, au motif que Facebook a présenté cette demande en retard pour une telle contestation et qu'elle dispose d'un autre recours adéquat dans l'exercice de son droit de répondre à la demande en cours du Commissariat présentée aux termes de l'alinéa 15a) de la LPRPDE (Facebook 1).

La Cour fédérale a entendu ces motions les 19 et 21 janvier 2021 et rendu sa décision le 15 juin 2021. En ce qui concerne la motion de Facebook visant à faire radier de grandes parties de l'affidavit du Commissariat, la Cour n'a pas été convaincue que la preuve par affidavit du Commissariat était inadmissible. Elle a conclu que seuls quelques paragraphes de l'affidavit et pièces déposées en preuve devaient être radiés. La Cour a également rejeté notre demande visant à exclure l'avis de demande de contrôle judiciaire déposé par Facebook. Elle a statué qu'il y avait à tout le moins une question discutable quant à savoir si Facebook disposait d'un autre recours adéquat sous le régime de la LPRPDE, si bien que les arguments de Facebook n'étaient pas dénués de toute chance de justifier l'exclusion de la demande à cette étape.

En février 2022, les parties ont terminé le contre-interrogatoire des témoins concernant les affidavits déposés dans la demande au titre de l'article 15 de la LPRPDE et dans la procédure de contrôle judiciaire. Le 11 avril 2022, Facebook a présenté ses observations à la Cour dans la procédure de contrôle judiciaire. Le Commissariat a présenté à la Cour ses observations en réponse à ces dernières le 28 avril 2022.

Dans la demande au titre de l'article 15 de la LPRPDE, le Commissariat a présenté une motion en vue de déposer une preuve par affidavit supplémentaire en mai 2022. Dans cette motion, le Commissariat demandait de plus à la Cour, ou subsidiairement, d'exiger que le déclarant de Facebook réponde aux questions auxquelles il avait refusé de répondre lors du contre-interrogatoire, dont le nombre s'élevait à plus de 70. L'audience s'est déroulée à Toronto sur deux jours, soit le 30 mai 2022 et le 10 juin 2022. Selon l'ordonnance de la Cour, la déclarante de Facebook doit se rendre disponible pour être réinterrogée par le Commissariat relativement à certaines questions soulevées lors du contre-interrogatoire initial. La Cour s'est également prononcée sur le bien-fondé des questions du Commissariat et sur les refus de Facebook. Par ailleurs, elle a rejeté la demande du Commissariat de déposer une preuve supplémentaire par affidavit; toutefois, le Commissariat a obtenu l'autorisation de déposer une nouvelle demande à la suite du contre-interrogatoire, qui a pris fin le 26 juillet 2022.

Le Commissariat a déposé son dossier de demande au titre de l'article 15 de la LPRPDE sur le fond de l'affaire le 19 août 2022.

La Cour a ordonné que la demande de contrôle judiciaire et la demande au titre de l'article 15 de la LPRPDE soient entendues consécutivement, devant le même juge. Les dates d'audience n'ont pas encore été fixées.

Renvoi visant Google (A-250-21) (Cour d'appel fédérale)

La procédure de renvoi visant à déterminer si le moteur de recherche de Google est assujetti à la LPRPDE s'est poursuivie au cours de l'exercice. En 2018, le Commissariat avait présenté, en vertu de l'article 18.3 de la *Loi sur les Cours fédérales*, une demande de renvoi de deux questions pour audition et jugement. Ces questions ont été soulevées dans le contexte d'une plainte déposée par un individu alléguant que Google contrevient à la LPRPDE en continuant d'afficher de manière visible des liens menant à des articles de presse en ligne le concernant dans les résultats lorsque l'on fait une recherche à partir de son nom au moyen du service de moteur de recherche de l'entreprise. Le plaignant a demandé à Google de retirer les articles en question des résultats de recherches concernant son nom.

Voici les questions posées :

Dans l'exploitation de son service de moteur de recherche, est-ce que Google LLC (Google) recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales, au sens de l'alinéa 4(1)a) de la LPRPDE, lors de l'indexation de pages Web et de la présentation des résultats de recherches concernant le nom d'un individu?

L'exploitation du service de moteur de recherche de Google est-elle exclue du champ d'application de la partie 1 de la LPRPDE, selon les termes de l'alinéa 4(2)c) de la LPRPDE, parce que par une telle exploitation Google recueille, utilise et communique des renseignements personnels à des fins journalistiques, artistiques ou littéraires et à aucune autre fin?

En juillet 2021, la Cour fédérale a rendu sa décision sur les mérites des questions posées dans le renvoi. Elle s'est dite d'accord avec la position du Commissariat selon laquelle la LPRPDE s'applique au service de moteur de recherche de Google. La Cour a répondu par l'affirmative à la première question : lorsqu'elle exploite son service de moteur de recherche, Google recueille, utilise et communique des renseignements personnels dans le cadre d'activités commerciales. La Cour a répondu par la négative à la deuxième question : l'exploitation du service de moteur de recherche de Google n'est pas exclue du champ d'application de la LPRPDE et n'est pas admissible à l'exception prévue à l'alinéa 4(2)c) de cette loi, car l'entreprise ne l'exploite pas à des fins journalistiques, et certainement pas strictement à de telles fins.

Le 28 septembre 2021, Google a présenté un avis d'appel en vue d'obtenir une ordonnance visant à faire invalider les questions posées dans le renvoi ou à refuser d'y répondre – invoquant le motif qu'il n'est pas possible ou qu'il n'y a pas lieu de répondre à ces questions sans établir si une obligation éventuelle de retirer les liens de ses résultats de recherches contreviendrait à l'alinéa 2b) de la *Charte canadienne des droits et libertés* – ou, subsidiairement, une ordonnance répondant par l'affirmative à la deuxième question du renvoi.

Le Commissariat, le procureur général du Canada et le plaignant participent à l'appel à titre d'intimés. De plus, la Cour d'appel fédérale a aussi autorisé la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko et une coalition de médias canadiens à participer à l'audience en tant qu'intervenants.

L'audience relative à l'appel devrait avoir lieu en octobre 2022.

Cain c. Canada (ministre de la Santé) (T-645-20 et T-641-20) et Hayes c. Canada (ministre de la Santé) (T-637-20)

Sous réserve de certaines conditions et à la suite de leur inscription auprès de Santé Canada, les utilisateurs de cannabis médical peuvent produire eux-mêmes leur cannabis ou désigner quelqu'un qui le produira pour eux. Santé Canada a reçu des demandes d'information concernant ces inscriptions au titre de la *Loi sur l'accès à l'information*, notamment des demandes de renseignements comme les trois premiers caractères du code postal des producteurs à des fins personnelles qui sont inscrits. Selon la position adoptée par ce ministère, il devrait communiquer uniquement le premier caractère des codes postaux, car l'utilisation d'une portion plus complète de ces codes accroîtrait de façon inacceptable le risque de communication de renseignements concernant des individus identifiables.

Les renseignements personnels ne peuvent être communiqués, à moins que certaines exceptions ne s'appliquent. Les renseignements sont considérés comme des renseignements personnels lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources. (*Gordon c. Canada [ministre de la Santé]*, 2008 CF 258, paragraphe 34).

La commissaire à l'information du Canada était en désaccord avec la position de Santé Canada. Au nom des plaignants, elle a demandé la publication des trois premiers caractères du code postal des producteurs à des fins personnelles inscrits et des personnes désignées inscrites lorsqu'il n'y a pas de fortes probabilités que les individus puissent être identifiés.

Le Commissariat est intervenu dans cette affaire afin de recommander un cadre pour la mise en œuvre du critère visant à déterminer s'il y a de fortes probabilités d'identification des individus. Nous attendons toujours la décision de la Cour dans cette affaire.

Clearview AI - Contestations judiciaires

Le 2 février 2021, au terme de leur enquête, le Commissariat à la protection de la vie privée du Canada ainsi que la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta ont conclu que Clearview AI (Clearview) avait enfreint les lois provinciales et fédérale sur la protection des renseignements personnels applicables au secteur privé en prélevant des images dans Internet sans autorisation.

Cette entreprise américaine a constitué et gère une base de données d'images prélevées dans Internet sans le consentement des intéressés. La base de données, qui renfermait plus de 3 milliards d'images au moment de l'enquête, en compte maintenant plus de 20 milliards. Les clients de Clearview, dont faisait partie la Gendarmerie royale du Canada auparavant, sont en mesure de mettre en correspondance les photographies d'individus avec les images que renferme la base de données en se servant de la technologie de reconnaissance faciale.

En juillet 2020, Clearview avait informé les autorités canadiennes chargées de la protection de la vie privée qu'en réponse à leur enquête conjointe, elle n'offrira plus ses services de reconnaissance faciale au Canada. Ces données ont été principalement utilisées au Canada à des fins policières, mais à l'insu des intéressés et sans leur consentement. Ainsi, des milliards de personnes se sont trouvées à participer à des séances d'identification policière. Nous avons conclu que cette pratique représentait une surveillance de masse et contrevenait manifestement à la LPRPDE.

Clearview a invoqué une série d'arguments en s'appuyant sur le libellé de la LPRPDE, selon lequel il faut trouver un équilibre entre le droit à la vie privée et les intérêts commerciaux. D'après l'entreprise, les personnes qui avaient elles-mêmes versé leurs images dans Internet, ou permis qu'elles le soient, n'avaient plus d'attente raisonnable en matière de vie privée. Clearview affirmait qu'il s'agissait de renseignements auxquels le public avait accès et que ses intérêts commerciaux légitimes et sa liberté d'expression devaient prévaloir.

En décembre 2021, nos homologues provinciaux ont ordonné à Clearview de se conformer aux recommandations formulées à l'issue de l'enquête conjointe. Le Commissariat était en accord

avec les ordonnances provinciales, mais la LPRPDE ne lui confère aucun pouvoir de rendre des ordonnances.

Les ordonnances provinciales ayant force exécutoire obligent Clearview à :

- cesser d'offrir les services de reconnaissance faciale qui ont fait l'objet de l'enquête dans les trois provinces;
- cesser de recueillir, d'utiliser et de communiquer des images de personnes dans les trois provinces sans le consentement des individus;
- supprimer les images et les matrices faciales biométriques qui ont été recueillies auprès des individus dans les trois provinces sans leur consentement.

Clearview conteste ces ordonnances provinciales[1] devant les tribunaux (par voie de contrôle judiciaire) en faisant valoir, entre autres, les arguments suivants :

1) elle n'est pas assujettie aux lois provinciales sur la protection des renseignements personnels;
2) le public avait accès aux renseignements personnels en question, lesquels ont été recueillis, utilisés et communiqués de façon raisonnable;
3) certains articles des lois provinciales sur la protection des renseignements personnels contreviennent à l'alinéa 2b) de la *Charte canadienne des droits et libertés*;
4) il est impossible de se conformer aux ordonnances provinciales telles qu'elles sont formulées (c.-à-d. qu'elles sont déraisonnables et inapplicables).

Pour l'instant, notre rapport de conclusions d'enquête conjoint n'est pas contesté devant les tribunaux.

Le 16 septembre 2021, un avis de demande[2] de recours collectif au titre du paragraphe 14(1) de la LPRPDE a été déposé devant la Cour fédérale pour le groupe suivant : « toutes les personnes physiques, qui sont résidents ou citoyens du Canada et dont le visage apparaît sur les photographies recueillies par Clearview » [traduction]. Entre autres choses, ce recours collectif vise à obtenir :

- une déclaration de la Cour selon laquelle Clearview a recueilli, copié, mis en mémoire, utilisé et communiqué illégalement des renseignements personnels des membres du groupe et ainsi porté atteinte à leur droit à la vie privée;
- une ordonnance enjoignant à Clearview de détruire tous les renseignements personnels des membres du groupe et lui interdisant de commercialiser ou de fournir ses services au Canada;
- diverses formes de dommages-intérêts pour avoir porté atteinte à la vie privée des membres du groupe.

Le 30 novembre 2021, Clearview a réagi en déposant un « avis de question constitutionnelle » dans cette affaire. Elle conteste la validité constitutionnelle de la Partie I de la LPRPDE.

---

[1] À la Cour suprême de la Colombie-Britannique (le 14 janvier 2022) : No S-220204; devant la Cour du Banc de la Reine de l'Alberta (le 21 janvier 2022) : No 2201 01019; devant la Cour du Québec [Division administrative et d'appel] (le 14 janvier 2022) : No 500-80-042393-224.

[2] À la Cour fédérale du Canada (le 15 septembre 2021) : No de dossier de la Cour : T-1410-21.

Clearview conteste également la constitutionnalité de l'alinéa 7(1)d), des sous-alinéas 7(2)c.1) et 7(3)h.1) de la *Loi* ainsi que l'alinéa 1e) du *Règlement précisant les renseignements auxquels le public a accès*, DORS/2001-7. En résumé, Clearview semble faire valoir que la LPRPDE est invalide en vertu du paragraphe 94(1) de la *Loi constitutionnelle* et doit être déclarée inconstitutionnelle en vertu de l'article 52 de cette loi. La Cour fédérale n'a pas encore autorisé ce recours collectif ni confirmé les questions constitutionnelles. Le Commissariat suit de près l'évolution de cette affaire.

Annexes

Annexe 1 : Définitions

Types de plaintes

Accès

À la suite d'une demande officielle d'accès à l'information, l'institution ou l'organisation aurait refusé à une ou à plusieurs personnes l'accès aux renseignements personnels qu'elle détient à leur sujet.

Avis de prorogation

En vertu de la LPRP, l'institution n'aurait pas donné une justification appropriée pour la prorogation, aurait fait la demande de prorogation après le délai initial de 30 jours ou aurait fixé l'échéance à plus de 60 jours après la date de réception de la demande.

Collecte

L'institution ou l'organisation aurait recueilli des renseignements personnels non nécessaires ou les aurait recueillis par des moyens inéquitables ou illicites.

Consentement

En vertu de la LPRPDE, une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement valable de la personne en cause ou, pour le motif qu'elle fournit un bien ou un service, a exigé que la personne consente à une collecte, à une utilisation ou à une communication déraisonnable de renseignements personnels.

Conservation et retrait

L'institution ou l'organisation n'aurait pas conservé des renseignements personnels selon le calendrier de conservation pertinent – les renseignements auraient été détruits trop rapidement ou conservés trop longtemps.

Correction ou annotation (accès)

L'institution ou l'organisation n'aurait pas corrigé des renseignements personnels ou, en cas de désaccord avec les corrections demandées, n'aurait pas annoté le dossier pour en faire état.

Correction ou annotation (délais)

En vertu de la LPRP, l'institution n'aurait pas corrigé les renseignements personnels ou n'aurait pas annoté le dossier en conséquence dans les 30 jours suivant la réception de la demande de correction.

Délais

L'institution n'aurait pas répondu à une demande dans les délais prescrits par la LPRP.

Détermination des fins de la collecte des renseignements

En vertu de la LPRPDE, une organisation n'a pas déterminé les fins de la collecte de renseignements personnels avant la collecte ou au moment de celle-ci.

Exactitude

L'institution ou l'organisation n'aurait pas pris toutes les mesures raisonnables pour s'assurer que les renseignements personnels utilisés sont exacts, à jour et complets.

Frais

L'institution ou l'organisation aurait exigé indûment des frais pour répondre à une demande d'accès à des renseignements personnels.

Langue

En réponse à une demande présentée en vertu de la LPRP, l'institution n'aurait pas fourni les renseignements personnels dans la langue officielle choisie par le demandeur.

Mesures de protection

En vertu de la LPRPDE, une organisation n'a pas protégé par des mesures de protection appropriées les renseignements personnels qu'elle détient.

Possibilité de porter plainte

En vertu de la LPRPDE, une organisation n'a pas mis en place des procédures ou des politiques permettant à une personne de porter plainte à l'égard du non-respect de la Loi ou elle a enfreint ses propres procédures et politiques.

Répertoire

InfoSource (un répertoire du gouvernement fédéral qui décrit chaque institution et les banques de données – groupes de fichiers sur le même sujet – qu'elle possède) ne décrirait pas de façon adéquate le fonds de renseignements personnels d'une institution.

Responsabilité

En vertu de la LPRPDE, une organisation ne s'est pas acquittée de ses responsabilités à l'égard des renseignements personnels en sa possession ou sous sa garde ou elle n'a pas désigné une personne responsable de s'assurer qu'elle se conforme à la Loi.

Transparence

En vertu de la LPRPDE, une organisation n'a pas rendu facilement accessibles aux demandeurs des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Utilisation et communication

L'institution ou l'organisation aurait utilisé ou communiqué des renseignements personnels sans le consentement de la personne en cause ou les aurait utilisés ou communiqués de façon non conforme aux usages et aux communications prévus par la loi.

Décisions

Fondée

L'institution ou l'organisation a enfreint une disposition de la LPRP ou de la LPRPDE.

Fondée et résolue

L'institution ou l'organisation a enfreint une disposition de la LPRP ou de la LPRPDE, mais elle a par la suite pris des mesures correctives pour remédier à la situation à la satisfaction du Commissariat.

Fondée et conditionnellement résolue

L'institution ou l'organisation a enfreint une disposition de la LPRP ou de la LPRPDE. L'institution ou l'organisation s'est engagée à mettre en œuvre des mesures correctives satisfaisantes approuvées par le Commissariat.

Non fondée

L'enquête n'a pas mis au jour des éléments de preuve suffisants pour conclure que l'institution ou l'organisation a enfreint une loi sur la protection des renseignements personnels.

Résolue

En vertu de la LPRP, l'enquête a révélé que la plainte découle essentiellement d'une mauvaise communication, d'un malentendu, etc., entre les parties, et/ou l'institution a accepté de prendre des mesures pour remédier à la situation à la satisfaction du Commissariat.

Réglée

Le Commissariat a aidé à négocier en cours d'enquête une solution satisfaisante pour toutes les parties en cause et n'a publié aucune conclusion.

Abandonnée

En vertu de la LPRP : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. Diverses raisons peuvent entraîner l'abandon d'un dossier, mais ce ne peut être à la demande du Commissariat. Par exemple, il est possible que le plaignant ne veuille plus poursuivre la démarche ou que l'on ne puisse trouver ses coordonnées afin qu'il fournisse des renseignements supplémentaires essentiels pour en arriver à une conclusion.

En vertu de la LPRPDE : L'enquête a pris fin sans qu'une conclusion n'ait été publiée. Le commissaire peut mettre fin à l'enquête à sa discrétion pour un motif prévu au paragraphe 12.2(1) de la LPRPDE.

Hors du champ d'application

On a déterminé qu'aucune loi fédérale sur la protection des renseignements personnels ne s'applique à l'institution ou à l'organisation ou ne régit l'objet de la plainte. Par conséquent, le Commissariat ne produit aucun rapport.

Règlement rapide (RR)

La situation a été réglée à la satisfaction du plaignant dès le début du processus d'enquête. Le Commissariat n'a publié aucune conclusion.

Refus d’enquêter

En vertu de la LPRPDE, le commissaire a refusé d’amorcer l’examen d’une plainte, car il estime :

- que le plaignant aurait d’abord dû épuiser les recours internes ou les procédures d’appel ou de règlement des griefs qui lui sont normalement offerts;
- que la plainte pourrait avantageusement être instruite selon d’autres procédures prévues par le droit fédéral ou provincial; ou,
- que la plainte n’a pas été déposée dans un délai raisonnable après que son objet a pris naissance, comme le prévoit l’article 12(1) de la LPRPDE.

Retrait

En vertu de la LPRPDE, le plaignant a retiré sa plainte volontairement ou ne pouvait plus être joint dans les faits. Le Commissariat ne publie aucun rapport.

Annexe 2 : Tableaux statistiques

Tableaux relatifs à la LPRP

Tableau 1 - Décisions sur les plaintes relatives à l'accès et à la protection des renseignements personnels en vertu de la LPRP, par institution fédérale

Intimé	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Total
Administration canadienne de la sûreté du transport aérien								1	1
Affaires mondiales Canada				2				1	3
Agence canadienne d'inspection des aliments				1	1				2
Agence de la santé publique du Canada				1					1
Agence des services frontaliers du Canada	2		8	10				5	25
Agence du revenu du Canada	2		5	16		1		3	27
Agriculture et Agroalimentaire Canada				2					2
Anciens Combattants Canada			1	1			1		3
Banque du Canada	1								1
Bibliothèque et Archives Canada				1					1
Bureau du Conseil privé				2					2
Centre de la sécurité des télécommunications				2					2
Commissariat à l'information du Canada		2							2
Commissariat à l'intégrité du secteur public du Canada		1							1
Commission canadienne de sûreté nucléaire				1					1
Commission canadienne des droits de la personne				3					3

Commission civile d'examen et de traitement des plaintes relatives à la GRC			1	1					2
Commission de l'assurance-emploi du Canada				1					1
Commission de l'immigration et du statut de réfugié du Canada				2					2
Commission des libérations conditionnelles du Canada			1	7				1	9
Commission des relations de travail et de l'emploi dans le secteur public fédéral					1				1
Conseil canadien des relations industrielles				1					1
Conseil de la radiodiffusion et des télécommunications canadiennes				1					1
Défense nationale			1	18			1		20
École de la fonction publique du Canada							1	2	3
Élections Canada	1								1
Élections Canada / Bureau du directeur général des élections	1		1						2
Emploi et Développement social Canada	2	1	4	14		1			22
Énergie atomique du Canada limitée				1					1
Environnement et Changement climatique Canada			1						1
Exportation et développement Canada				1					1
Gendarmerie royale du Canada	7		18	46		3	3	1	78
Gouvernement fédéral du Canada	1								1
Immigration, Réfugiés et Citoyenneté Canada			3	18					21
Innovation, Sciences et Développement économique Canada				1	1				2
Ministère de la Justice	2		4	2					8
Office Canada-Terre-Neuve-et-Labrador des hydrocarbures extracôtiers				1					1
Office de surveillance des activités en matière de sécurité nationale et de renseignement				1					1
Parcs Canada			2						2

Pêches et Océans Canada		1	1	2				1	5
Relations Couronne-Autochtones et Affaires du Nord Canada			1						1
Ressources naturelles Canada				1					1
Santé Canada	1			4					5
Secrétariat du Conseil du Trésor du Canada				1					1
Service canadien d'appui aux tribunaux administratifs			1	2		2			5
Service canadien du renseignement de sécurité			4	6					10
Service correctionnel Canada	1		15	29		12	1	3	61
Services aux Autochtones Canada				2					2
Services partagés Canada				4					4
Services publics et Approvisionnement Canada	1		1	18					20
Société canadienne des postes			1	11		1		1	14
Société Radio-Canada				1					1
Statistique Canada			2	3	1				6
Téléfilm Canada				1					1
Transports Canada			1	3					4
Total	**22**	**5**	**77**	**246**	**4**	**20**	**7**	**19**	**400**

Tableau 2 - Délais de traitement des plaintes en vertu de la LPRP – Règlement rapide, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen en mois
Protection des renseignements personnels	**121**	**5,17**
Exactitude	1	6,13
Collecte	18	4,58
Conservation et retrait	7	4,21
Utilisation et communication	95	5,34
Accès	**117**	**6,31**
Accès	114	6,39
Correction ou annotation	3	3,23
Délais	**81**	**0,99**
Correction – Délais	1	4,49
Délais	80	0,95
Total	**319**	**4,53**

Tableau 3 - Délais de traitement des plaintes en vertu de la LPRP – Enquêtes officielles, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen en mois
Protection des renseignements personnels	**63**	**15,90**
Collecte	11	17,54
Conservation et retrait	2	24,79
Utilisation et communication	50	15,19
Accès	**99**	**15,54**
Accès	97	15,78
Correction ou annotation	2	3,58
Délais	**312**	**2,91**
Avis de prorogation	1	1,54
Délais	311	2,91
Total	**474**	**7,27**

Tableau 4 - Délais de traitement des plaintes en vertu de la LPRP – Tous les dossiers fermés, par décision

Type de plainte	Nombre	Délai de traitement moyen en mois
Règlement rapide	**319**	**4,53**
Enquêtes officielles	**474**	**7,28**
Abandonnée	28	16,76
Hors du champ d'application	5	27,63
Non fondée	81	11,38
Résolue	8	11,39
Réglée	4	55,51
Fondée	20	11,80
Fondée et conditionnellement résolue	108	3,86
Fondée - Présomption de refus	54	3,70
Fondée et résolue	166	4,54
Total	**793**	**6,17**

Tableau 5 - Atteintes en vertu de la LPRP, par institution

Intimé	Nombre
Affaires mondiales Canada	6
Agence canadienne d'inspection des aliments	1
Agence de la santé publique du Canada	2
Agence des services frontaliers du Canada	1
Agence du revenu du Canada	7
Anciens Combattants Canada	3
Autorité du Pont Windsor-Detroit	2
Bureau du vérificateur général du Canada	1
Commissariat aux langues officielles	2
Commission canadienne des droits de la personne	1
Commission de l'immigration et du statut de réfugié du Canada	1
Commission de la capitale nationale	1
Commission de la fonction publique	8
Conseil national de recherches Canada	2
Défense nationale	1
Emploi et Développement social Canada	349
Gendarmerie royale du Canada	13
GRC du Gouvernement du Canada	1
Immigration, Réfugiés et Citoyenneté Canada	6
Office de surveillance des activités en matière de sécurité nationale et de renseignement	1
Pêches et Océans Canada	1
Régie de l'énergie du Canada	3
Santé Canada	1
Service Canada	1
Service correctionnel Canada	36
Services partagés Canada	1
Services publics et Approvisionnement Canada	2
Société canadienne des postes	2
Statistique Canada	3
Téléfilm Canada	2
Transports Canada	2
Total	**463**

Tableau 6 - Plaintes et atteintes en vertu de la LPRP

Catégorie	Total
Acceptées	
Protection des renseignements personnels	306
Accès	247
Délais	353
Total des plaintes acceptées	**906**
Fermées à la suite d'un règlement rapide	
Protection des renseignements personnels	121
Accès	117
Délais	81
Total	**319**
Fermées à la suite d'une enquête officielle	
Protection des renseignements personnels	63
Accès	99
Délais	312
Total	**474**
Total des dossiers fermés	**793**
Atteintes signalées	
Communication non autorisée*	132
Perte	279
Vol	11
Accès non autorisé	41
Total des atteintes signalées	**463**

* Au cours des exercices précédents, le terme « communication accidentelle » était utilisé pour désigner les cas où des renseignements personnels avaient été communiqués en dehors des dispositions de la LPRP. Ce terme a été remplacé par « communication non autorisée », conformément aux Lignes directrices sur les atteintes à la vie privée du SCT, mais le sens demeure le même.

Tableau 7 - Plaintes en vertu de la LPRP acceptées, par type de plainte

Type de plainte	Règlement rapide		Enquête sommaire**		Enquête officielle		Total	
	Nombre	Pourcentage*	Nombre	Pourcentage*	Nombre	Pourcentage*	Nombre	Pourcentage*
Accès								
Accès	194	43 %	17	6 %	31	19 %	242	27 %
Correction ou annotation	4	1 %	1	0 %	1	1 %	6	1 %
Délais								
Correction – Délais	1	0 %					1	0 %
Avis de prorogation			1	0 %			1	0 %
Délais	82	18 %	269	93 %			351	39 %
Protection des renseignements personnels								
Exactitude	3	1 %					3	0 %
Collecte	34	7 %	1	0 %	58	36 %	93	10 %
Conservation et retrait	6	1 %			1	1 %	7	1 %
Utilisation et communication	131	29 %	1	0 %	70	43 %	202	22 %
Total	**455**	**100 %**	**290**	**100 %**	**161**	**100 %**	**906**	**100 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

** Les enquêtes sommaires sont des enquêtes plus courtes qui se soldent par la publication d'un bref rapport ou d'une lettre de conclusions.

Tableau 8 - Les 10 institutions fédérales visées par le plus grand nombre de plaintes acceptées en vertu de la LPRPDE

Intimé	Protection des renseignements personnels			Accès			Délais			Total
	Règlement rapide	Enquête sommaire	Enquête officielle	Règlement rapide	Enquête sommaire	Enquête officielle	Règlement rapide	Enquête sommaire	Enquête officielle	
Service correctionnel Canada	33	1	4	43	4	1	3	93		182
Gendarmerie royale du Canada	20		3	34	4	2	38	78		179
Agence des services frontaliers du Canada	8		8	12	1		6	18		53
Défense nationale	5		6	12			10	20		53
Immigration, Réfugiés et Citoyenneté Canada	17		4	7		2	5	14		49
Agence du revenu du Canada	7		4	22	1	5	5	4		48
Société canadienne des postes	5		33	2		2	1	2		45
Emploi et Développement social Canada	13		3	4		2		4		26
Services publics et Approvisionnement Canada	6		2	6		2	1	2		19
Service canadien du renseignement de sécurité	1		1	7	4	1				14
Total	**115**	**1**	**68**	**149**	**14**	**17**	**69**	**235**	**0**	**668**

Tableau 9 - Les 10 institutions fédérales visées par le plus grand nombre de plaintes acceptées en vertu de la LPRP par année fiscale

Intimé	2017-18	2018-19	2019-20	2020-21	2021-22
Service correctionnel Canada	440	426	155	130	182
Gendarmerie royale du Canada	232	273	176	186	179
Agence des services frontaliers du Canada	76	109	42	48	53
Défense nationale	93	121	33	51	53
Immigration, Réfugiés et Citoyenneté Canada	29	59	44	47	49
Agence du revenu du Canada	63	79	63	40	48
Société canadienne des postes	33	29	4	22	45
Emploi et Développement social Canada	24	39	25	41	26
Services publics et Approvisionnement Canada	49	27	70	42	19
Service canadien du renseignement de sécurité	26	24	15	16	14
Total	**1065**	**1186**	**627**	**623**	**668**

Tableau 10 - Plaintes en vertu de la LPRP acceptées, par institution

Intimé	Règlement rapide	Enquête sommaire	Enquête officielle	Total
Administration canadienne de la sûreté du transport aérien	1		1	2
Affaires mondiales Canada	5	5	1	11
Agence canadienne d’inspection des aliments	1		2	3
Agence de la santé publique du Canada	3	2	7	12
Agence des services frontaliers du Canada	26	19	8	53
Agence d'évaluation d'impact du Canada	3			3
Agence du revenu du Canada	34	5	9	48
Agence spatiale canadienne			1	1
Agriculture et Agroalimentaire Canada	1			1
Anciens Combattants Canada	10	2	1	13
Banque de développement du Canada			1	1
Bibliothèque et Archives Canada	3	1		4
Bureau de la sécurité des transports du Canada			2	2
Bureau de l'enquêteur correctionnel	1	1		2

Bureau du Conseil privé	4	1	1	6
Bureau du vérificateur général du Canada			2	2
Centre d'analyse des opérations et déclarations financières du Canada			1	1
Centre de la sécurité des télécommunications	1	5	2	8
Commissariat à l'information du Canada			1	1
Commissariat aux langues officielles	2			2
Commission canadienne des droits de la personne	6	1		7
Commission civile d'examen et de traitement des plaintes relatives à la GRC	1			1
Commission de l'immigration et du statut de réfugié du Canada	1	1	1	3
Commission de la fonction publique	2		1	3
Commission des libérations conditionnelles du Canada	5	1	1	7
Conseil canadien des relations industrielles	1			1
Conseil de la radiodiffusion et des télécommunications canadiennes	1			1
Conseil de recherches en sciences humaines	1			1
Conseil de recherches en sciences naturelles et en génie du Canada	1	3		4
Conseil national de recherches Canada			1	1
Défense nationale	27	20	6	53
École de la fonction publique du Canada		2		2
Élections Canada / Bureau du directeur général des élections	4			4
Emploi et Développement social Canada	17	4	5	26
Énergie atomique du Canada limitée			1	1
Environnement et Changement climatique Canada	1	1		2
Exportation et développement Canada	1			1
Gendarmerie royale du Canada	92	82	5	179
Gouvernement fédéral du Canada			4	4
Immigration, Réfugiés et Citoyenneté Canada	29	14	6	49
Innovation, Sciences et Développement économique Canada	3	1	1	5
Ministère de la Justice	4	2	4	10
Ministère des Finances Canada			2	2
Musée canadien de la nature		1		1

Office Canada-Terre-Neuve-et-Labrador des hydrocarbures extracôtiers	1			1
Office de surveillance des activités en matière de sécurité nationale et de renseignement	1		1	2
Parcs Canada	1		1	2
Patrimoine canadien	1	1		2
Pêches et Océans Canada	6	1	5	12
Relations Couronne-Autochtones et Affaires du Nord Canada	9	1		10
Ressources naturelles Canada	2			2
Santé Canada	6	1	6	13
Secrétariat du Conseil du Trésor du Canada	1		4	5
Sécurité publique Canada	2		3	5
Service canadien d'appui aux tribunaux administratifs	5		2	7
Service canadien du renseignement de sécurité	8	4	2	14
Service correctionnel Canada	79	98	5	182
Service des poursuites pénales du Canada		1		1
Services aux Autochtones Canada	3		4	7
Services partagés Canada	2		3	5
Services publics et Approvisionnement Canada	13	2	4	19
Société canadienne des postes	8	2	35	45
Société immobilière du Canada Limitée			1	1
Société Radio-Canada	2		1	3
Statistique Canada	5	3	1	9
Téléfilm Canada	1			1
Trans Mountain Corporation	2			2
Transports Canada	4	2	4	10
Tribunal des anciens combattants (révision et appel)	1			1
VIA Rail Canada			1	1
Total	**455**	**290**	**161**	**906**

Tableau 11 - Décisions en vertu de la LPRP, par province, territoire ou autres

Province, territoire ou autres	Règlement rapide		Enquête sommaire		Enquête officielle		Total	
	Nombre	Pourcentage*	Nombre	Pourcentage*	Nombre	Pourcentage*	Nombre	Pourcentage*
Colombie-Britannique	110	24,18 %	67	23,10 %	20	12,42 %	197	21,74 %
Alberta	51	11,21 %	37	12,76 %	11	6,83 %	99	10,93 %
Saskatchewan	2	0,44 %	11	3,79 %	5	3,11 %	18	1,99 %
Manitoba	8	1,76 %	4	1,38 %	2	1,24 %	14	1,55 %
Ontario	155	34,07 %	104	35,86 %	74	45,96 %	333	36,75 %
Québec	84	18,46 %	43	14,83 %	36	22,36 %	163	17,99 %
Nouveau-Brunswick	18	3,96 %	9	3,10 %	4	2,48 %	31	3,42 %
Nouvelle-Écosse	12	2,64 %	8	2,76 %	4	2,48 %	24	2,65 %
Île-du-Prince-Édouard	1	0,22 %		0,00 %		0,00 %	1	0,11 %
Terre-Neuve-et-Labrador	6	1,32 %	3	1,03 %	2	1,24 %	11	1,21 %
États-Unis	1	0,22 %	1	0,34 %		0,00 %	2	0,22 %
Autres (excluant les États-Unis)	6	1,32 %	3	1,03 %	1	0,62 %	10	1,10 %
Non précisé	1	0,22 %		0,00 %	2	1,24 %	3	0,33 %
Total	**455**	**100 %**	**290**	**100 %**	**161**	**100 %**	**906**	**100 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 12 - Décisions en vertu de la LPRP, par type de plainte

Type de plainte	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée - Présomption de refus	Fondée et résolue	Total
Protection des renseignements personnels										
Exactitude				1						1
Collecte	2		5	18	1	1	2			29
Conservation et retrait	2			7						9
Utilisation et communication	9	1	15	98	3	14	5			145
Accès										
Accès	9	4	55	119		5			19	211
Correction ou annotation			2	3						5
Délais										
Correction – Délais				1						1
Avis de prorogation			1							1
Délais	6		3	80			101	54	147	391
Total	**28**	**5**	**81**	**327**	**4**	**20**	**108**	**54**	**166**	**793**

Tableau 13 - Décisions sur les plaintes relatives aux délais en vertu de la LPRP, par institution

Intimé	Abandonnée	Non fondée	Résolue	Fondée et conditionnellement résolue	Fondée - Présomption de refus	Fondée et résolue	Total
Affaires mondiales Canada			1	1	3	2	7
Agence de la santé publique du Canada				1	1	1	3
Agence des services frontaliers du Canada			6	6	8	7	27
Agence d'évaluation d'impact du Canada			1				1
Agence du revenu du Canada			3			4	7
Agence fédérale de développement économique pour le Sud de l'Ontario						1	1
Anciens Combattants Canada			4	3			7
Bibliothèque et Archives Canada			1			1	2
Bureau de la sécurité des transports du Canada				1			1
Bureau de l'enquêteur correctionnel			1			1	2
Bureau du Conseil privé						1	1
Centre de la sécurité des télécommunications				1	2	1	4
Commission canadienne des droits de la personne			1			1	2
Commission de l'immigration et du statut de réfugié du Canada		1					1
Conseil de recherches en sciences naturelles et en génie du Canada				3			3
Défense nationale			10	11	3	8	32
École de la fonction publique du Canada				1		1	2
Emploi et Développement social Canada		1		2	2	1	6
Environnement et Changement climatique Canada			1	1		2	4
Gendarmerie royale du Canada	3		37	11	16	50	117

Immigration, Réfugiés et Citoyenneté Canada	1		5	1	1	11	19
Innovation, Sciences et Développement économique Canada			1		1	2	4
Ministère de la Justice						1	1
Musée canadien de la nature						1	1
Patrimoine canadien						1	1
Pêches et Océans Canada		1	1				2
Santé Canada			1			1	2
Secrétariat du Conseil du Trésor du Canada				1	2		3
Sécurité publique Canada			1	1			2
Service correctionnel Canada	1		3	55	14	42	115
Service des poursuites pénales du Canada						1	1
Services aux Autochtones Canada			1				1
Services publics et Approvisionnement Canada			1			4	5
Société canadienne des postes		1	1				2
Statistique Canada					1		1
Trans Mountain Corporation						1	1
Transports Canada	1			1			2
Total	**6**	**4**	**81**	**101**	**54**	**147**	**393**

Tableaux relatifs à la LPRPDE

Tableau 1 - Plaintes en vertu de la LPRPDE acceptées*, par secteur de l'industrie

Secteur de l'industrie	Nombre	Proportion de l'ensemble des plaintes acceptées*
Agriculture, foresterie, chasse et pêche	2	0 %
Aliments et boissons	6	1 %
Assurances	25	6 %
Construction	1	0 %
Divertissement	6	1 %
Édition (sauf Internet)	6	1 %
Fabrication	8	2 %
Finances	102	24 %
Gouvernement	4	1 %
Hébergement	41	10 %
Individuel	2	0 %
Internet	44	10 %
Location	3	1 %
Organismes sans but lucratif	2	0 %
Professionnels	22	5 %
Santé	11	3 %
Services	32	7 %
Services publics	1	0 %
Télécommunications	53	12 %
Transports	28	7 %
Ventes et détail	28	7 %
Total	**427**	**100 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 2 - Plaintes en vertu de la LPRPDE acceptées*, par type de plainte

Type de plainte	Nombre	Proportion de l'ensemble des plaintes acceptées
Accès	121	28 %
Collecte	57	13 %
Consentement	19	4 %
Conservation	36	8 %
Correction ou annotation	4	1 %
Délais	13	3 %
Exactitude	2	0 %
Mesures de protection	19	4 %
Transparence	1	0 %
Responsabilité	1	0 %
Utilisation et communication	154	36 %
Total	**427**	**100 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 3 - Dossiers d'enquête liés à la LPRPDE fermés, par secteur de l'industrie et décision

Secteur de l'industrie	Réglée rapidement	Refusée	Abandonnée (article 12.2)	Hors du champ d'application	Non fondée	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Retrait	Total
Agriculture, foresterie, chasse et pêche	1										1
Aliments et boissons	1										1
Assurances	23		3		1						27
Construction	1										1
Divertissement	3	1									4
Édition (sauf Internet)	11		2			1					14
Fabrication	9									1	10
Finances	68		3		3		5		3	2	84
Gouvernement	3										3
Hébergement	19				1						20
Individu	2										2
Internet	34									1	35
Non précisé	1										1
Organismes sans but lucratif			1								1
Professionnels	12		1			1			1		15
Santé	3			1				1			5
Services	31		5		2			1	1	2	42
Services publics	1										1
Télécommunications	33		3		2			1			39
Transports	18		1					1			20
Ventes et détail	29		2		1						32
Total	**303**	**1**	**21**	**1**	**10**	**2**	**5**	**4**	**5**	**6**	**358**

Tableau 4 - Dossiers d'enquête en vertu de la LPRPDE fermés par type de plainte et décision

Type de plainte	Réglée rapidement	Refusée	Abandonnée (article 12.2)	Hors du champ d'application	Non fondée	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Retrait	Total
Accès	94		4		2		1		3	1	105
Collecte	29		3		2	1					35
Consentement	23	1	3	1	2		1	1		3	35
Conservation	28										28
Correction ou annotation	1										1
Délais	5							1		1	7
Exactitude	2									1	3
Fins acceptables									1		1
Mesures de protection	16		5		1		1	1	1		25
Utilisation et communication	105		6		3	1	2	1			118
Total	**303**	**1**	**21**	**1**	**10**	**2**	**5**	**4**	**5**	**6**	**358**

Tableau 5 - Enquêtes en vertu de la LPRPDE – Délais de traitement moyens, par décision

Décision	Nombre	Délai de traitement moyen, en mois
Résolue par règlement rapide	303	6,3
Refusée	1	14,0
Abandonnée (article 12.2)	21	9,9
Hors du champ d'application	1	13,8
Non fondée	10	13,0
Réglée	2	5,1
Fondée	5	21,1
Fondée et conditionnellement résolue	4	32,7
Fondée et résolue	5	32,0
Retrait	6	16,9
Total	**358**	
Moyenne générale pondérée		**7,8**

Tableau 6 - Enquêtes en vertu de la LPRPDE– Délais de traitement moyens, par type de plainte et de règlement

Type de plainte	Règlement rapide		Autres règlements		Toutes les enquêtes	
	Nombre	Délai de traitement moyen, en mois	Nombre	Délai de traitement moyen, en mois	Nombre	Délai de traitement moyen, en mois
Accès	94	6,7	11	12,8	105	7,4
Collecte	29	7,4	6	11,8	35	8,2
Consentement	23	8,7	12	16,6	35	11,4
Correction ou annotation	1	6,7			1	6,7
Délais	5	0,8	2	2,2	7	1,2
Exactitude	2	4,1	1	46,4	3	18,2
Fins acceptables			1	69,0	1	69,0
Conservation	28	5,9			28	5,9
Mesures de protection	16	7,8	9	18,8	25	11,7
Utilisation et communication	105	5,3	13	13,4	118	6,2
Total	**303**	**6,3**	**55**	**15,9**	**358**	**7,8**

Tableau 7 - Déclarations des atteintes en vertu de la LPRPDE, par secteur de l'industrie et type d'incident

Secteur	Type d'incident				Total des incidents par secteur	Proportion de l'ensemble des incidents**
	Perte	Vol	Accès non autorisé	Communication non autorisée*		
Agriculture, foresterie, chasse et pêche			2		2	0 %
Aliments et boissons			4		4	1 %
Assurances	15	3	36	35	89	14 %
Construction			4		4	1 %
Divertissement			5	1	6	1 %
Édition (sauf Internet)			6	1	7	1 %
Extraction minière et extraction de pétrole et de gaz			5	1	6	1 %
Fabrication	1	1	48	3	53	8 %
Finances	14	11	71	35	131	20 %
Gouvernement			10	4	14	2 %
Hébergement		1	2		3	0 %
Internet			6	3	9	1 %
Location			1		1	0 %
Organismes sans but lucratif	1	1	18	6	26	4 %
Professionnels	4	2	53	21	80	12 %
Santé	4		12	6	22	3 %
Services	1		17	12	30	5 %
Services publics			2	1	3	0 %
Télécommunications	1	2	61	27	91	14 %
Transports			12		12	2 %
Ventes et détail	2		44	6	52	8 %
Total	**43**	**21**	**419**	**162**	**645**	**100 %**

* Au cours des exercices précédents, le terme « communication accidentelle » était utilisé pour désigner les cas où des renseignements personnels avaient été communiqués en dehors des dispositions de la LPRPDE, que ce soit intentionnellement ou accidentellement. Ce terme a été remplacé par « communication non autorisée », conformément au libellé de la LPRPDE, mais le sens demeure le même.
** Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 8 - Nombre de comptes canadiens touchés par type d'incident

Type d'incident	Nombre de comptes touchés
Accès non autorisé	1 916 557
Communication non autorisée*	21 605
Perte	2 869
Vol	5 077
Total	**1 946 108**

* Au cours des exercices précédents, le terme « communication accidentelle » était utilisé pour désigner les cas où des renseignements personnels avaient été communiqués en dehors des dispositions de la LPRPDE, que ce soit intentionnellement ou accidentellement. Ce terme a été remplacé par « communication non autorisée », conformément au libellé de la LPRPDE, mais le sens demeure le même.

Annexe 3 : Lois essentiellement similaires

En vertu du paragraphe 25(1) de la LPRPDE, le Commissariat doit déposer chaque année au Parlement un rapport « sur la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires ».

En vertu de l'alinéa 26(2)b) de la LPRPDE, le gouverneur en conseil peut, par décret, exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de cette loi à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur d'une province ayant adopté une loi provinciale « essentiellement similaire ».

Le 3 août 2002, Industrie Canada (maintenant connu sous le nom d'Innovation, Sciences et Développement économique Canada) a publié le Processus de détermination du caractère « essentiellement similaire » d'une loi provinciale par le gouverneur en conseil. On y présente la politique et les critères utilisés pour déterminer si une loi provinciale sera considérée comme essentiellement similaire. En vertu de la politique, les lois essentiellement similaires :

- fournissent un mécanisme de protection des renseignements personnels conforme et équivalent à celui de la LPRPDE;
- intègrent les 10 principes de l'annexe 1 de la LPRPDE;
- fournissent un mécanisme indépendant et efficace de surveillance et de recours ainsi que des pouvoirs d'enquête;
- restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées et légitimes.

Les organisations assujetties aux lois provinciales réputées essentiellement similaires sont exemptées de la LPRPDE en ce qui a trait à la collecte, à l'utilisation et à la communication de renseignements personnels à l'intérieur de la province visée. La LPRPDE continue toutefois de s'appliquer à la collecte, à l'utilisation ou à la communication de renseignements personnels liée aux activités d'entreprises fédérales dans la province visée ainsi qu'à la collecte, à l'utilisation ou à la communication de renseignements personnels à l'extérieur de cette province.

Les lois provinciales considérées comme essentiellement similaires sont les suivantes :

- *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec;
- *Personal Information Protection Act* de la Colombie-Britannique;
- *Personal Information Protection Act* de l'Alberta;
- *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario (dépositaires de renseignements sur la santé);
- *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick (dépositaires de renseignements sur la santé);
- *Personal Health Information Act* de Terre-Neuve-et-Labrador (dépositaires de renseignements sur la santé); et,
- *Personal Health Information Act* de la Nouvelle-Écosse (dépositaires de renseignements sur la santé).

Annexe 4 : Rapport de la commissaire spéciale à la protection de la vie privée

L'an dernier, un nombre peu élevé de dossiers m'ont été présentés aux fins d'examen. Dans tous les cas, il s'agissait de plaintes que je ne pouvais accepter comme recevables, car le sujet ne relevait pas de ma compétence.

Les personnes en cause dans les dossiers examinés cherchaient néanmoins à obtenir de l'aide. J'ai pu cerner leurs préoccupations et les diriger dans la bonne direction pour poursuivre leurs démarches. Dans certains cas, j'en ai informé directement le Commissariat à la protection de la vie privée du Canada, si ce dernier était déjà intervenu dans le dossier.

Dans un cas en particulier, je n'ai pas été en mesure d'établir la véritable nature des questions en jeu. La personne, qui cherchait réellement à en appeler de certaines décisions, faisait référence à plusieurs dossiers actifs, en cours ou fermés. J'ai donc demandé des précisions au Commissariat concernant ces dossiers et, une fois les renseignements obtenus, j'ai pu expliquer à la personne la façon de procéder. Même s'il ne relevait pas de ma compétence d'examiner les questions en cause, j'ai toutefois été en mesure de rendre service à cette personne ainsi qu'aux autres qui m'ont écrit l'an dernier.

En tant que commissaire spéciale à la protection de la vie privée, j'ai le pouvoir d'enquêter sur toute plainte qui pourrait être déposée contre le Commissariat en vertu de la *Loi sur la protection des renseignements personnels*. Par exemple, lorsqu'une demande d'accès à des renseignements personnels est présentée au Commissariat et que celui-ci la refuse, le demandeur est alors en droit de déposer une plainte auprès de la commissaire spéciale. Une autre forme de plainte peut être déposée lorsqu'il est soutenu que le Commissariat a traité les renseignements personnels d'une personne d'une manière inappropriée, qui serait contraire à la *Loi sur la protection des renseignements personnels*, à laquelle est assujetti le Commissariat. Je n'ai reçu aucune plainte de cette nature l'an dernier.

Je compte continuer, au cours de l'année à venir, d'être au service de ceux qui solliciteront mon intervention.

Le tout respectueusement soumis,

Anne E. Bertrand, c.r.
Commissaire spéciale