



Quatrième rapport d'étape sur les évolutions en matière de législation sur la protection des données au Canada

Rapport à la Commission européenne, décembre 2018

Cette publication est également offerte en ligne http://www.ic.gc.ca/eic/site/113.nsf/fra/h_07664.html

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication : www.ic.gc.ca/demande-publication ou communiquer avec:

Centre de services Web
Innovation, Sciences et Développement économique Canada
Édifice C.D. Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5
Canada

Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
TTY (pour les personnes malentendantes) : 1-866-694-8389
Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)
Courriel : ISDE@Canada.ca

Autorisation de reproduction

À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission du ministère de l'Industrie, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, que le ministère de l'Industrie soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec le ministère de l'Industrie ou avec son consentement.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, veuillez demander l'affranchissement du droit d'auteur de la Couronne : www.ic.gc.ca/demande-droitdauteur ou communiquer avec le Centre de services Web aux coordonnées ci-dessus.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de l'Industrie, (2018).

N° de catalogue Iu37-8/4-2019F-PDF

ISBN 978-0-660-29319-6

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

Also available in English under the title *Fourth Update Report on Developments in Data Protection Law in Canada*.

Table des matières

1.0	Introduction	1
2.0	Évolutions en matière de législation sur la protection des renseignements personnels dans le secteur privé	1
3.0	Initiatives législatives	3
4.0	Activités des comités parlementaires	6
5.0	Activités du Commissariat à la protection de la vie privée	7
6.0	Autres sujets d'intérêt	9
7.0	Coordonnées	11
	Annexe – Renseignements supplémentaires	12

1.0 Introduction

1.1 En décembre 2001, la Commission européenne (CE) a rendu la Décision 2002/2/CE, en vertu du paragraphe 25(6) de la Directive 95/46/CE. La Décision énonce que le Canada est considéré comme assurant un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne (UE) aux destinataires assujettis à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). La décision d'adéquation a été réaffirmée en 2006.

1.2 Conformément à l'article 2 de la Décision d'exécution (UE) 2016/2295, qui a modifié la Décision 2002/2/CE, la CE est maintenant tenue de suivre, de manière permanente, les évolutions du cadre juridique canadien, y compris les évolutions concernant l'accès des autorités publiques aux données à caractère personnel, afin d'évaluer si le Canada continue d'assurer un niveau de protection adéquat des données à caractère personnel.

1.3 En mai 2017, dans le cadre de ses efforts continus pour aider la Commission à s'acquitter de ses obligations de surveillance, les responsables du gouvernement du Canada ont transmis aux responsables de la CE le premier d'une série de rapports semestriels qui traitent des évolutions du cadre canadien de la protection des données¹.

1.4 L'obligation de surveillance de la CE a été réaffirmée en mai 2018 par l'application du paragraphe 45(4) du *Règlement général sur la protection des données* (RGPD), qui oblige la Commission, de façon continue, à surveiller les évolutions liées à la vie privée au Canada susceptibles d'avoir une incidence sur le fonctionnement de la décision d'adéquation existante. Reconnaisant que cette activité de surveillance se poursuit, dans le cadre de l'évaluation et de l'examen du RGPD, qui doit inclure un examen des décisions existantes en matière d'adéquation, qui a lieu tous les quatre ans, à compter de mai 2020, le présent rapport :

- précise les évolutions du cadre de protection des données au Canada depuis le troisième rapport d'étape préparé en juin 2018;
- donne, en annexe, de plus amples renseignements sur les sujets d'intérêt soulevés par les responsables de la CE lors de la vidéoconférence tenue le 12 septembre 2018.

2.0 Évolutions en matière de législation sur la protection des renseignements personnels dans le secteur privé

Règlement sur les atteintes aux mesures de sécurité en vertu de la LPRPDE

2.1 Le 1^{er} novembre 2018, de nouvelles dispositions de la [Loi sur la protection des renseignements personnels et les documents électroniques](#) (LPRPDE) relatives aux atteintes aux mesures de sécurité et le [Règlement sur les atteintes aux mesures de sécurité](#) sont entrées en vigueur. À ce titre, la LPRPDE exige maintenant des organisations qu'elles avisent les personnes touchées et qu'elles signalent au Commissariat à la protection de la vie privée (CPVP) toutes les atteintes qui présentent un risque réel de

¹ La série de rapports semestriels à la CE est disponible à l'adresse <http://www.ic.gc.ca/eic/site/113.nsf/fra/home>.

préjudice important pour les personnes touchées. Les organisations doivent également tenir des registres de toute atteinte aux données dont elles prennent connaissance et les fournir au CPVP sur demande. Les organisations qui, sciemment, ne respectent pas ces obligations seront passibles d'amendes. Par exemple, les organisations qui n'avertissent pas volontairement les particuliers d'une atteinte qui crée un risque réel de préjudice important pourraient être passibles d'amendes pouvant aller jusqu'à 100 000 \$ CAN par personne non avisée. Ces nouvelles exigences visent à fournir aux particuliers la capacité de se protéger contre les préjudices causés par une atteinte et à inciter les organisations à offrir de meilleures mesures de sécurité des données. Le gouvernement a travaillé activement auprès des intervenants ces derniers mois afin de les sensibiliser davantage aux nouvelles obligations en matière d'atteinte aux données dans le cadre de la LPRPDE.

2.2 Le CPVP a élaboré un aperçu des nouvelles obligations liées à une atteinte aux mesures de sécurité. Le [document d'orientation](#) du CPVP fournit des renseignements à l'intention des entreprises sur la déclaration obligatoire des atteintes aux mesures de sécurité, y compris les infractions qui doivent être signalées au CPVP, les avis aux personnes touchées ainsi que les obligations de tenue de registres.

Loi canadienne anti-pourriel

2.3 Le 11 juillet 2018, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a pris des mesures coercitives contre l'installation de logiciels malveillants par l'entremise de publicités en ligne en vertu de la *Loi canadienne anti-pourriel* (LCAP). Le CRTC a signifié des procès-verbaux de violation à Datablocks et à Sunlight Media pour avoir prétendument aidé à installer des programmes informatiques malveillants (maliciels) par la distribution de publicités en ligne. Les entreprises sont tenues de payer 100 000 \$ CAN et 150 000 \$ CAN respectivement en sanctions administratives pécuniaires à la suite de l'enquête².

2.4 Le 4 octobre 2018, le CRTC a signé un protocole d'entente³ avec l'Organe des régulateurs européens des communications électroniques (ORECE) pour établir une relation de coopération. Grâce à ce protocole d'entente, les deux organismes appuieront leurs efforts respectifs pour relever les défis actuels et futurs en matière de réglementation au Canada et en Europe ainsi que pour établir des relations de travail collégiales. Ils se concentreront sur un certain nombre de grands thèmes, y compris l'accès de prochaine génération et le développement de la large bande, la protection des consommateurs, l'éducation et l'autonomisation, la neutralité du réseau, Internet ouvert et la concurrence du marché. Le CRTC et l'ORECE entendent exercer leurs activités de coopération pendant une période de deux ans, qui pourrait être prolongée d'une autre période de deux ans.

2.5 Le 5 novembre 2018, le CRTC a publié le *Bulletin d'information de Conformité et Enquêtes 2018-415*⁴, qui fournit des lignes directrices générales sur la conformité et les pratiques exemplaires aux intervenants relativement à l'article 9 de la LCAP. Le *Bulletin* traite de l'approche

² L'enquête se trouve à l'adresse <https://crtc.gc.ca/fra/archive/2018/vt180711.htm> et le communiqué de presse connexe, à l'adresse <https://www.canada.ca/fr/radiodiffusion-telecommunications/nouvelles/2018/07/le-crtc-impose-des-penalites-totalisant-250000-pour-lutter-contre-les-publicites-en-ligne-malveillantes.html>.

³ Le texte du PE se trouve à l'adresse <https://crtc.gc.ca/fra/internet/berec.htm>.

⁴ Le bulletin 2018-415 du CRTC est disponible à l'adresse https://crtc.gc.ca/fra/archive/2018/2018-415.htm?_ga=2.144851056.536770588.1541431232-781512184.1525446427.

générale du CRTC concernant l'article 9 et présente des exemples de parties auxquelles le présent article pourrait s'appliquer et d'activités pouvant entraîner la non-conformité. Il propose également des mesures de gestion des risques connexes. Les articles 6 à 8 de la LCAP interdisent l'envoi de messages électroniques commerciaux sans consentement, la modification des données de transmission des messages électroniques dans le cadre d'une activité commerciale sans consentement et l'installation d'un programme informatique sur l'ordinateur d'une autre personne dans le cadre d'une activité commerciale sans consentement. L'article 9 de la LCAP traite des façons dont les personnes peuvent contribuer aux contraventions des articles 6 à 8 de la LCAP sans commettre les violations directement.

3.0 Initiatives législatives

Projet de loi C-59, Loi concernant des questions de sécurité nationale, 2017

3.1 Le gouvernement du Canada a déposé le projet de loi C-59, *Loi concernant des questions de sécurité nationale*⁵, qui renforcerait les mécanismes de responsabilisation des organismes de sécurité nationale et modifierait les pouvoirs du Service canadien du renseignement de sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST). Le projet de loi a été étudié par le Comité permanent de la sécurité nationale de la Chambre des communes et a été renvoyé à la Chambre des communes, avec modifications, en mai 2018. En décembre 2018, le projet de loi a été renvoyé au Comité sénatorial permanent de la sécurité nationale et de la défense pour étude.

3.2 Le projet de loi propose un Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), qui remplacerait et renforcerait les fonctions d'examen du Comité de surveillance des activités de renseignement de sécurité (CSARS) et du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST). À l'heure actuelle, les organismes d'examen de la sécurité nationale du Canada fonctionnent séparément, chacun étant responsable d'un organisme de renseignement de sécurité. En vertu du projet de loi C-59, l'OSSNR sera en mesure d'examiner les activités de sécurité nationale de tout ministère ou organisme gouvernemental ayant une fonction de sécurité nationale, y compris le SCRS, le CST, Affaires mondiales Canada, l'Agence des services frontaliers du Canada et Sécurité publique Canada. Cela élargit considérablement la portée de l'activité gouvernementale qui fait l'objet d'un examen et renforce la capacité du système canadien d'examen de la sécurité nationale de suivre l'information qui circule entre les ministères et les organismes qui ont des activités liées à la sécurité nationale. En outre, les ministres pourront demander à l'OSSNR d'examiner les activités qui se rapportent à la sécurité nationale ou au renseignement de sécurité entreprises par leur ministère ou organisme. L'OSSNR enquêtera sur les plaintes déposées contre le SCRS et le CST ainsi que sur les plaintes concernant la conduite de la GRC lorsque ces plaintes sont fondées sur des questions relatives à la sécurité nationale.

⁵ De plus amples renseignements sur le projet de loi C-59, *Loi concernant des questions de sécurité nationale*, sont disponibles à l'adresse <http://www.parl.ca/LegisInfo/BillDetails.aspx?Language=F&billId=9057418>.

3.3 Le processus de plaintes de l'OSSNR proposé fonctionnera comme celui de son organisme prédécesseur, le CSARS. En ce qui concerne le processus de dépôt d'une plainte à l'OSSNR⁶ par un particulier, la procédure restera sensiblement la même. En ce qui concerne le SCRS et le CST, le plaignant doit d'abord déposer une plainte auprès de l'organisation. S'il n'est pas satisfait de la réponse, ou s'il n'en a pas reçu dans un délai raisonnable, il peut déposer une plainte devant l'OSSNR.

3.4 Outre sa fonction de plainte, l'OSSNR peut examiner toute activité relative à la sécurité nationale ou au renseignement de sécurité et doit examiner la mise en œuvre de toutes les directives ministérielles fournies au SCRS et au CST ou à d'autres ministères lorsque ces directives se rapportent à sécurité nationale ou au renseignement de sécurité. Ces directives servent d'instructions de haut niveau aux ministères et aux organismes et orientent la mise en œuvre des activités du ministère ou de l'organisme. Une fois l'examen terminé, l'OSSNR peut formuler des constatations ou recommandations qu'il jugera appropriées, y compris en ce qui concerne le respect de la loi ou des directives ministérielles, ou le caractère raisonnable et la nécessité de l'exercice de pouvoirs par un ministère du gouvernement.

3.5 L'OSSNR publiera un rapport annuel public sur ses activités cette année-là, y compris les versions non classifiées de ses constatations et recommandations, en assurant la transparence et la surveillance publique des activités des ministères et organismes gouvernementaux. Si, au cours d'un examen, elle estime qu'une activité liée à la sécurité nationale ou au renseignement de sécurité n'est pas conforme à la Loi, l'OSSNR doit présenter un rapport au ministre responsable.

3.6 En 2017, la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (CPSNR) a été promulguée, créant un comité multipartite qui examine le cadre législatif, réglementaire, stratégique, administratif et financier de la sécurité nationale et du renseignement. Le mandat du CPSNR ne comprend pas l'enquête sur les plaintes. Le Comité se concentre sur les questions primordiales qui traitent de la façon dont les ministères et les organismes de sécurité nationale du Canada s'acquittent de leur mandat. Le Comité peut également examiner toute activité liée à la sécurité nationale ou au renseignement, à moins que cette activité ne fasse partie d'une opération en cours ou ne porterait atteinte à la sécurité nationale.

Projet de loi C-21, Loi modifiant la Loi sur les douanes

3.7 En juin 2016, le gouvernement canadien a déposé une loi modifiant la *Loi sur les douanes* en vertu du projet de loi C-21, *Loi modifiant la Loi sur les douanes*⁷. Le projet de loi autorise l'ASFC à recueillir des renseignements personnels sur toute personne qui quitte ou a quitté le Canada à tous les points d'entrée terrestres. De plus, il exige que toute personne qui quitte le Canada se présente, si on le lui demande, à un agent et réponde à ses questions. Il modifie la Loi pour autoriser la communication de renseignements douaniers à un fonctionnaire du ministère de l'Emploi et du Développement social aux fins de l'application ou de l'exécution de la *Loi sur la sécurité de la vieillesse* (en plus de la *Loi sur*

⁶ Toute personne peut déposer une plainte auprès de l'OSSNR au sujet des mesures de sécurité nationale prises par un ministère ou un organisme du gouvernement canadien, qu'elle réside ou non au Canada. Le processus de plainte est le même indépendamment de la nationalité.

⁷ De plus amples renseignements sur le projet de loi C-21, *Loi modifiant la Loi sur les douanes*, sont disponibles à l'adresse <http://www.parl.ca/LegisInfo/BillDetails.aspx?Language=F&billId=8355229>

l'assurance-emploi). Enfin, elle modifie la Loi pour autoriser les agents à exiger que les marchandises qui doivent être exportées du Canada soient déclarées et examinées malgré toute exemption prévue par la Loi. Le 23 octobre 2018, le projet de loi C-21 a franchi l'étape de la deuxième lecture au Sénat et a été renvoyé au Comité sénatorial permanent de la sécurité nationale et de la défense. Le projet de loi confère l'autorisation législative de recueillir des renseignements personnels conformément à l'article 4 de la *Loi sur la protection des renseignements personnels* et prescrit la durée de conservation de ces renseignements.

Projet de loi C-58, Loi modifiant la Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels et d'autres lois en conséquence

3.8 Le 19 juin 2017, le gouvernement présentait un projet de loi visant à modifier la *Loi sur l'accès à l'information* (LAI) et à apporter des modifications corrélatives à la *Loi sur la protection des renseignements personnels*. Le projet de loi C-58 représente la première phase d'une approche en deux étapes de l'examen de la LAI fédérale. La deuxième phase, qui consiste à moderniser la Loi, comprendra un examen complet de la Loi devant commencer dans l'année suivant son entrée en vigueur. Le projet de loi propose de nouvelles exigences pour la publication proactive d'un large éventail d'informations qui s'appliquent à 265 institutions du gouvernement fédéral ainsi qu'au Cabinet du premier ministre, aux cabinets des ministres et aux organes administratifs qui appuient le Parlement et les tribunaux. Le projet de loi propose aussi de transformer le rôle du commissaire à l'information de celui d'une autorité dotée du pouvoir législatif de rendre une ordonnance concernant le traitement des demandes, y compris la publication de documents. Il offrirait aussi au commissaire à l'information la possibilité de consulter le commissaire à la protection de la vie privée en ce qui concerne l'application de l'exemption en vertu de la LAI qui contraint les institutions fédérales à refuser de communiquer des documents renfermant des renseignements personnels. Un examen de la LAI serait également exigé tous les cinq ans.

3.9 Le projet de loi modifierait la *Loi sur la protection des renseignements personnels* afin de maintenir la cohérence entre les deux lois concernant les exigences en matière de déclaration, le partage des services de traitement des demandes et le pouvoir du gouverneur en Conseil de mettre à jour la liste des institutions gouvernementales assujetties à la Loi. La version actuelle du projet de loi a été adoptée par la Chambre des communes le 6 décembre 2017 et elle se trouve maintenant devant le Sénat.

Projet de loi C-76, Loi sur la modernisation des élections, 2018

3.10 Le 30 avril 2018, le gouvernement a présenté la *Loi sur la modernisation des élections*⁸, qui propose de modifier la *Loi électorale du Canada* et d'autres lois pour mettre à jour les systèmes électoraux et politiques du Canada et régler les problèmes posés par l'ère numérique, y compris les préoccupations concernant la collecte et l'utilisation de données par les partis politiques. Le projet de loi exigerait que les partis politiques créent et publient une politique décrivant comment ils entendent

⁸ De plus amples renseignements sur le projet de loi C-76, *Loi sur la modernisation des élections*, sont disponibles à l'adresse <http://www.parl.ca/LegisInfo/BillDetails.aspx?billId=9808070&Language=F>.

protéger la vie privée des électeurs, y compris les renseignements qu'ils recueillent auprès des électeurs potentiels et la façon dont ils seront sauvegardés et utilisés. Le 22 octobre 2018, le Comité permanent de la procédure et des affaires de la Chambre a renvoyé le projet de loi à la Chambre des communes avec des modifications qui exigeraient que les plateformes en ligne publient des registres des messages de publicité partisane et électorale qu'elles publient. Le projet de loi a ensuite franchi l'étape de la troisième lecture le 30 octobre 2018 et a été renvoyé au Sénat, où le Comité sénatorial permanent des affaires juridiques et constitutionnelles l'étudie.

4.0 Activités des comités parlementaires

Étude sur l'atteinte à la sécurité des renseignements personnels impliquant Cambridge Analytica et Facebook

4.1 Le 22 mars 2018, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) a adopté une motion pour mener une étude au sujet des répercussions sur la vie privée des monopoles de plateforme et des possibles recours réglementaires et législatifs nationaux et internationaux visant à assurer la confidentialité des données des citoyens et l'intégrité des processus démocratiques et électoraux à travers le monde. Le 19 juin 2018, le Comité a publié un rapport provisoire sur son étude⁹. Le Comité a repris ses activités le 25 septembre 2018 et entend formuler des recommandations additionnelles dans son rapport définitif une fois l'étude terminée.

Rapport du Sénat sur les véhicules automatisés

4.2 Le 29 janvier 2018, le Comité sénatorial permanent des transports et des communications a publié son rapport, intitulé *Paver la voie : Technologie et le futur du véhicule automatisé*, à la suite d'une étude sur les questions réglementaires et techniques liées au déploiement de véhicules connectés et automatisés (VCA), que le Comité avait commencée en mars 2016. Le rapport contient seize recommandations sur des questions liées aux VCA, dont plusieurs liées à la protection de la vie privée telles que l'évaluation de la nécessité de règles de confidentialité propres aux VCA. La réponse du gouvernement¹⁰ au rapport du Comité sénatorial, qui a été déposée le 27 juillet 2018, souscrit en grande partie aux recommandations du Comité relatives à la protection de la vie privée et prend note de l'étude complémentaire de la LPRPDE par la Chambre des communes¹¹. Le gouvernement s'est également engagé à collaborer avec les intervenants et les partenaires, y compris le Commissariat à la protection de la vie privée, afin d'élaborer un code des pratiques exemplaires en matière de protection de la vie privée propre à l'industrie.

⁹ De plus amples renseignements sur l'étude du Comité sur l'atteinte à la sécurité des renseignements personnels impliquant Cambridge Analytica et Facebook sont disponibles à l'adresse <http://www.ourcommons.ca/Committees/fr/ETHI/StudyActivity?studyActivityId=10044891>.

¹⁰ Disponible à l'adresse https://sencanada.ca/content/sen/committee/421/TRCM/reports/MinisterGarneau_GovResp_b.pdf.

¹¹ Voir l'examen de la LPRPDE du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique intitulée [Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques](#) et la [Réponse du gouvernement](#) connexe.

5.0 Activités du Commissariat à la protection de la vie privée

Questions administratives

5.1 Plus tôt cette année, le commissaire fédéral à la protection de la vie privée a fait plusieurs annonces pour indiquer que le Commissariat à la protection de la vie privée avait adopté une nouvelle structure organisationnelle¹². Ce nouveau cadre est basé sur deux domaines de programme : la conformité et la promotion. Le programme de conformité a pour but de régler les problèmes existants de conformité en matière de protection de la vie privée par le recours à diverses activités d'application de la loi pour veiller à ce qu'on détecte les infractions et recommande des mesures correctives. Cela comprendra des enquêtes sur les plaintes déposées par des particuliers ainsi qu'une réorientation vers une mise en application plus proactive, comme la tenue d'enquêtes ou le lancement de vérifications par le commissaire. Le programme de promotion vise à informer les particuliers de leurs droits et de la façon de les exercer et à rendre les organisations plus conformes aux lois fédérales sur la protection des renseignements personnels. Cela comprend l'élaboration et la promotion d'information et de conseils pratiques; l'examen et la préparation de commentaires sur les évaluations des facteurs relatifs à la vie privée (EFVP); et la collaboration proactive avec le gouvernement et l'industrie à titre consultatif afin de mieux comprendre et d'atténuer les incidences sur la vie privée liées aux nouvelles technologies telles que les mégadonnées, l'intelligence artificielle et l'Internet des objets.

Rapport annuel au Parlement

5.2 Le 27 septembre 2018, le Commissariat a déposé au Parlement son rapport annuel 2017-2018 sur la LPRPDE et la *Loi sur la protection des renseignements personnels*¹³. Dans ce rapport, le commissaire mentionne les enquêtes en cours sur un certain nombre d'atteintes récentes au droit à la vie privée, y compris celles impliquant Cambridge Analytica et Facebook, Uber et Equifax.

Réputation en ligne/Google

5.3 En janvier 2018, le CPVP a publié son *Projet de position sur la réputation en ligne*¹⁴ dans le cadre d'un processus de consultation publique relatif à la vie privée et à la réputation en ligne. Il y indique être d'avis que l'indexation des pages Web et l'affichage des résultats de recherche par les moteurs de recherche constituent des activités visées par la LPRPDE. Toutefois, il existe actuellement une certaine incertitude quant à cette interprétation de la loi à cet égard. Dans le cadre d'une enquête impliquant une personne qui allègue que Google contrevient à la LPRPDE, le Bureau a décidé de demander à la Cour fédérale de fournir des précisions quant à l'applicabilité de la LPRPDE.

5.4 Le 10 octobre 2018, le Commissariat à la protection de la vie privée a déposé un avis de requête à la Cour fédérale du Canada afin de déterminer si le moteur de recherche de Google est assujéti à la

¹² De plus amples renseignements sont fournis dans le Plan ministériel 2018-2019 du Commissariat à la protection de la vie privée du Canada, déposé au Parlement le 16 avril 2018 à l'adresse https://www.priv.gc.ca/fr/a-propos-du-commissariat/rapports-operationnels-du-commissariat/depenses-prevues-du-commissariat/dp-index/2018-2019/dp_2018-19/.

¹³ Le rapport est disponible à l'adresse https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201718/ar_201718/.

¹⁴ Le projet de position est disponible à l'adresse https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-sur-la-reputation-en-ligne/pos_or_201801/.

législation fédérale en matière de protection des renseignements personnels. Plus précisément, la demande de renvoi cherche à déterminer si le service de moteur de recherche de Google recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales et s'il est, de ce fait, assujéti à la LPRPDE. Il demande également si Google est exempté de la LPRPDE parce que ses fins sont exclusivement journalistiques ou littéraires. Le CPVP a annoncé que les enquêtes sur les plaintes relatives aux demandes de déréférencement seront suspendues en attendant les résultats du renvoi. Le Commissariat attendra également le point de vue de la Cour avant d'arrêter sa position sur la réputation en ligne.

Collecte de renseignements financiers par Statistique Canada

5.5 Le 31 octobre 2018, le commissaire à la protection de la vie privée a ouvert une enquête sur Statistique Canada à la suite de plaintes relatives à la collecte de renseignements personnels émanant d'organismes du secteur privé. Statistique Canada travaille sur de nouvelles façons de comprendre les consommateurs en ligne, la production des ménages, l'investissement immatériel et l'évolution des questions sociales et environnementales dans un monde de plus en plus numérisé. La *Loi sur la statistique* confère à l'organisme le pouvoir juridique de recueillir des données, celles-ci ne devant être utilisées qu'à des fins statistiques et sous réserve de fortes protections législatives. Comme la question était d'intérêt pour le Comité sénatorial permanent des banques et du commerce, dans le cadre d'une étude en cours sur l'état actuel du système financier national et international, le commissaire à la protection de la vie privée et les fonctionnaires de Statistique Canada ont été invités à comparaître devant le Comité¹⁵.

Résolution du commissaire à la protection de la vie privée sur le processus électoral

5.6 En septembre 2018, les ombudsmans et les commissaires à l'information et à la protection de la vie privée du Canada ont publié une résolution conjointe intitulée *Assurer la confidentialité dans le processus électoral du Canada*¹⁶. Dans la résolution, les commissaires fédéraux, provinciaux et territoriaux à la protection de la vie privée du Canada exhortent leurs gouvernements respectifs à veiller à ce que le droit canadien, à tous les niveaux, comporte des obligations de confidentialité significatives pour les partis politiques. La résolution appelle les gouvernements à adopter des lois qui : obligent les partis politiques à respecter les principes de protection des renseignements personnels et de la vie privée reconnus mondialement; s'assurent que les Canadiens ont le droit d'accéder aux renseignements personnels à leur sujet; et prévoient une surveillance indépendante pour vérifier la conformité à la vie privée et en assurer le respect par les partis politiques. La résolution porte sur le projet de loi C-76 (*Loi sur la modernisation des élections*), qui exigera que les partis politiques fédéraux inscrits élaborent des politiques en matière de protection des renseignements personnels et les publient en ligne.

¹⁵ De plus amples informations sont disponibles à l'adresse <https://sencanada.ca/fr/comites/BANC/Avisdeconvocation/505782/42-1>.

¹⁶ De plus amples informations sont disponibles à l'adresse https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_180913/.

6.0 Autres sujets d'intérêt

Stratégie nationale de données

6.1 Le greffier du Conseil privé a publié une feuille de route de la Stratégie de données pour la fonction publique fédérale¹⁷ qui vise à favoriser l'utilisation stratégique des données par le gouvernement tout en protégeant la vie privée des citoyens. Bien que les données n'aient pas toutes des incidences sur la vie privée, la Stratégie indique que lorsqu'elles en ont, les ministères et organismes devraient penser à la protection de la vie privée dès la conception et collaborer rapidement avec le Commissariat à la protection de la vie privée. La feuille de route vise à harmoniser les efforts internes du gouvernement de façon à utiliser les données de manière plus stratégique et complète d'autres travaux en cours, y compris les consultations nationales sur la transformation numérique et la transformation des données (voir ci-dessous).

Consultations nationales sur le numérique et les données

6.2 Le 19 juin 2018, le ministre de l'Innovation, des Sciences et du Développement économique Canada (ISDE) a lancé des consultations publiques sur le numérique et la transformation des données axées sur les domaines suivants : « Libérer la puissance de l'innovation », « L'avenir du travail » et « Confiance et respect de la vie privée ». Les [consultations nationales sur le numérique et les données](#) comprenaient un portail en ligne permettant à tous les Canadiens de participer à la discussion. Le processus a pris fin en octobre 2018 à la suite de consultations publiques nationales en ligne et d'une série de tables rondes dans les villes du Canada. Le gouvernement a l'intention de publier sous peu un rapport de type « ce que nous avons entendu ». Les résultats des consultations guideront les changements législatifs liés à la vie privée ainsi que d'autres cadres du marché.

Intelligence artificielle

6.3 Dans le contexte de sa présidence du G7 en 2018, le Canada continue de faire progresser le travail international sur l'intelligence artificielle. Dans la foulée de l'engagement pris par les ministres de l'innovation du G7 au cours de leur réunion ministérielle *Se préparer aux emplois de l'avenir*, le Canada a accueilli le 6 décembre 2018 à Montréal une conférence multipartite du G7 sur l'intelligence artificielle qui faisait fond sur la [Déclaration des ministres de l'innovation du G7 au sujet de l'intelligence artificielle](#) et la [Vision commune de Charlevoix sur l'avenir de l'intelligence artificielle](#) des leaders du G7. Cette conférence a rassemblé plus de 150 leaders de l'intelligence artificielle de l'ensemble du G7, y compris des représentants gouvernementaux, des universitaires, des membres de la société civile, des instituts de recherche, des partenaires du secteur privé et des experts, pour discuter de la façon de permettre l'adoption responsable de l'intelligence artificielle en insistant particulièrement sur la promotion de l'inclusion dans le développement et le déploiement de l'intelligence artificielle, la réduction des obstacles à l'innovation, le renforcement de la confiance des marchés, la responsabilisation par rapport à l'intelligence artificielle, la promotion d'une plus grande confiance sociétale et l'avenir du travail et des

¹⁷ La Stratégie de données est disponible à l'adresse <https://www.canada.ca/fr/conseil-prive/organisation/greffier/publications/strategie-donnees.html>.

compétences pour l'économie moderne, le tout en vue de bâtir une vision commune de l'intelligence artificielle centrée sur l'être humain.

6.4 Le 6 décembre 2018, le premier ministre du Canada et le secrétaire d'État de la France chargé du Numérique ont annoncé le mandat du Groupe international d'experts en intelligence artificielle (G2IA). Le G2IA favorisera la collaboration internationale en vue de promouvoir une compréhension commune de l'intelligence artificielle ainsi que d'appuyer et d'orienter l'adoption responsable d'une intelligence artificielle qui est centrée sur l'être humain et fondée sur les droits de la personne, l'inclusion, la diversité, l'innovation et la croissance économique. Au cours des prochains mois, le Canada et la France inviteront des partenaires internationaux partageant les mêmes idées à se joindre à eux pour faire du G2IA un point de référence mondial pour l'intelligence artificielle.

6.5 Le gouvernement a commencé à utiliser les technologies d'apprentissage machine pour améliorer les services et les programmes publics. Par exemple, pour faciliter le traitement du volume croissant de demandes de résidence temporaire, Immigration, Réfugiés et Citoyenneté Canada utilise l'analyse prédictive et la mise en œuvre de modèles pour aider les agents à déterminer les demandes qui sont routinières et simples afin de les traiter plus rapidement, pour trier les dossiers qui sont plus complexes afin de les examiner plus à fond et pour détecter la fraude ou d'autres méfaits dans certains secteurs d'activité. Ce projet d'analyse perfectionnée repose sur de solides fondements d'éthique et de respect de la vie privée tout au long du processus de développement de même que sur de multiples évaluations des facteurs relatifs à la vie privée. Des protocoles additionnels ont été mis en œuvre pour veiller à ce que l'évaluation soit approfondie et impartiale.

Internet des objets

6.6 La Société Internet, en collaboration avec la Clinique d'intérêt public et de politique Internet du Canada et ISDE, a lancé un processus multipartite canadien sur l'amélioration de la sécurité de l'Internet des objets (IdO). Le groupe a mis en place plusieurs groupes de travail pour aborder trois thèmes principaux :

- l'étiquetage des produits
- l'éducation et la sensibilisation des consommateurs
- la résilience du réseau

Bien qu'il en soit encore aux toutes premières étapes de ses travaux, le groupe fait des progrès constants vers un ensemble commun de normes volontaires. Le groupe entend rendre ces normes compatibles avec d'autres normes internationales pour les appareils IdO.

Autres engagements internationaux

6.7 Le Canada continue de participer à des instances internationales telles que l'Organisation de coopération et de développement économiques (OCDE) et le forum de la Coopération économique Asie-Pacifique (APEC) qui prennent activement part à des initiatives visant à améliorer et à étendre l'interopérabilité mondiale des cadres de protection de la vie privée. L'examen prochain des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère*

personnel (« Lignes directrices de protection de la vie privée ») de l'OCDE et les travaux entre l'APEC et la Commission européenne visant à étudier l'interopérabilité entre le système de règles transfrontalières de protection de la vie privée (RTPVP) de l'APEC et le *Règlement général sur la protection des données* (RGPD) de l'UE sont particulièrement importants. Le Canada participera activement au groupe consultatif d'experts de l'OCDE que l'on est à mettre en place pour soutenir l'examen des lignes directrices de l'OCDE sur la protection de la vie privée; il est aussi membre du groupe de travail de l'APEC qui a été constitué pour définir un programme de travail potentiel pour le renouvellement de la collaboration entre l'APEC et l'UE dans le contexte du RGPD.

7.0 Coordonnées

7.1 Pour de plus amples renseignements sur tout aspect du présent rapport, veuillez communiquer avec Charles Taillefer, directeur, Direction de la politique sur la vie privée et la protection des données, Direction générale des politiques-cadres du marché, Innovation, Sciences et Développement économique Canada, au 235, rue Queen, Ottawa (Ontario) K1A 0H5, Canada.

7.2 Les prochains rapports devraient paraître à intervalles réguliers, environ tous les six mois.

Annexe – Renseignements supplémentaires

La présente annexe donne de plus amples renseignements et détails au sujet des points qui ont été présentés dans le troisième rapport d'étape, lequel a été remis à la CE en juin 2018, mais dont il n'a pas été question dans le corps du présent rapport.

Commissaire au renseignement

A1.1 Le projet de loi C-59 énonce les fonctions et responsabilités de surveillance du commissaire au renseignement (CR). En vertu de la *Loi sur le commissaire au renseignement* proposée, le CR sera chargé d'examiner le caractère raisonnable des décisions ministérielles concernant l'utilisation de certains pouvoirs par le Service canadien du renseignement de sécurité (SCRS) et le Centre de la sécurité des télécommunications (CST). Le CR aura accès à tous les renseignements dont le ministre a été saisi. Le CR déterminera ensuite s'il était raisonnable pour le ministre d'avoir émis l'autorisation selon les preuves à l'appui.

A1.2 Le CR recevra des copies de tous les rapports de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et du Comité des parlementaires de la sécurité nationale et du renseignement (CPSNR) qui se rapportent à leurs attributions. Le CR fournira des copies de toutes ses décisions à l'OSSNR pour que celui-ci sache quelles mesures ont été jugées déraisonnables.

A1.3 En vertu de la *Loi sur le commissaire au renseignement*, le CR est nommé pour un mandat de cinq ans et a le pouvoir exclusif de gérer le personnel pour l'aider dans ses fonctions. Le CR fournit des copies de ses décisions aux organes de supervision de la sécurité nationale du Canada, faisant ainsi en sorte qu'ils soient dûment informés.

A1.4 Le CR aurait le mandat de superviser l'autorisation de certaines activités du SCRS et du CST et serait totalement indépendant du gouvernement. Le rôle du CR à l'égard du SCRS se limiterait à la surveillance de certaines activités bien précises du SCRS. Plus précisément, son rôle consisterait en ce qui suit :

- examiner et approuver les décisions du ministre concernant les catégories d'ensembles de données canadiens que le SCRS pourrait recueillir (article 16 de la *Loi sur le CR*);
- examiner et approuver les autorisations du ministre (ou de son délégué) pour la conservation d'ensembles de données étrangers (article 17 de la *Loi sur le CR*);
- dans des situations d'urgence, examiner et approuver l'autorisation du directeur du SCRS pour l'interrogation d'ensembles de données canadiens ou étrangers (article 18 de la *Loi sur le CR*);
- examiner et approuver les décisions du ministre concernant les catégories d'activités qui pourraient être entreprises en vertu du régime d'autorisation pour des actes ou des omissions qui constitueraient autrement des infractions.

Le CR évaluerait le caractère raisonnable de la décision du ministre (ou de son délégué) ou du directeur du SCRS d'autoriser de telles activités. En ce qui concerne le CST, le CR examinerait et évaluerait les autorisations ministérielles autorisant les activités de renseignement étranger et de cybersécurité. Le CR

examinerait les autorisations ministérielles pour s'assurer qu'elles sont raisonnables, nécessaires, proportionnées et que des protections appropriées en matière de vie privée sont en place.

A1.5 Le processus du commissaire du renseignement ajoutera un nouveau niveau de responsabilisation pour certains types d'activités du SCRS, notamment les activités pour lesquelles un mandat n'est pas exigé. Le CR évaluerait le caractère raisonnable de la décision du ministre compétent d'autoriser certaines activités de collecte spécifiées comme suit :

- Les autorisations de renseignement étranger (paragraphe 34(1) et 34(2)) émises en vertu du paragraphe 26(1) de la *Loi sur le CST*. Ces autorisations permettent au CST de recueillir des renseignements étrangers par l'entremise de l'infrastructure mondiale de l'information.
- Les autorisations de cybersécurité (paragraphe 34(1) et 34(3)) émises en vertu du paragraphe 27(1) ou 27(2) de la *Loi sur le CST*. Ces autorisations permettent au CST d'accéder à l'infrastructure d'information d'une institution fédérale afin de la protéger contre toute utilisation ou perturbation non autorisée, et ce, dans le but d'assurer la sécurité des institutions fédérales.
- Les activités du SCRS en vertu du paragraphe 20.1(3) et les activités du SCRS liées aux ensembles de données. Ces activités du SCRS peuvent également nécessiter un mandat, selon la nature de l'activité.

A1.6 Les décisions concernant les activités d'enquête assujetties au régime des mandats de l'article 21 de la *Loi sur le Service canadien du renseignement de sécurité (Loi sur le SCRS)* ne seront pas assujetties à l'examen additionnel du caractère raisonnable par le CR. Le régime des mandats et les fonctions du CR sont plutôt censés être des mécanismes de surveillance complémentaires ou distincts. Cependant, il peut y avoir certains domaines où l'on a recours aux deux. Par exemple, lors de l'exécution d'un mandat en vertu de l'article 21, le SCRS pourrait demander à la Cour fédérale de conserver des renseignements recueillis incidemment dans l'exécution du mandat pour constituer un ensemble de données. Si la Cour l'autorise, un tel ensemble de données serait alors assujetti au cadre de données de l'article 11 du projet de loi C-59, y compris les fonctions de supervision spécifiques du CR, comme indiqué ci-dessus. Il est important de noter que le SCRS est assujetti à un examen par le CSARS et le CPSNR et qu'il sera examiné par l'OSSNR proposé dans le projet de loi C-59.

Ensembles de données en vertu du projet de loi C-59

A1.7 Le projet de loi C-59 modifie également la *Loi sur le SCRS* pour créer un régime en application duquel le SCRS recueillera, conservera, interrogera et exploitera des ensembles de données qui contiennent des renseignements personnels qui ne se rapportent pas directement ou immédiatement à des activités qui représentent une menace pour la sécurité du Canada¹⁸. Cela donne au SCRS la capacité de poursuivre ses enquêtes en dégageant des liens et tendances que ne permettent pas de cerner les méthodes d'enquête traditionnelles. Le cadre définit trois types d'ensembles de données : les ensembles de données accessibles au public; les ensembles de données canadiens, qui se rapportent principalement aux Canadiens et aux personnes au Canada; et les ensembles de données étrangers, qui

¹⁸ Un cadre proposé est disponible à l'adresse <https://www.canada.ca/fr/services/defense/securitenationale/notre-securite-nos-droits/cadre-propose-ensembles-donnees-scrs.html>.

se rapportent principalement aux non-Canadiens à l'extérieur du Canada. Les ensembles de données étrangers ne peuvent être conservés que s'ils satisfont au seuil selon lequel ils sont susceptibles d'aider le SCRS dans l'exercice de ses fonctions. Leur conservation doit être autorisée par le ministre (ou son délégué) et approuvée par le CR pour une période pouvant aller jusqu'à cinq ans. L'accès aux ensembles de données étrangers est limité aux employés désignés et soumis à des exigences de tenue de registres et de vérification. Dans l'ensemble, l'approche proposée fournirait un cadre clair au sein duquel le SCRS pourrait procéder à l'analyse des données à l'aide d'ensembles de données qui ne sont pas directement liés aux menaces tout en veillant à ce que des mécanismes de protection et de responsabilisation appropriés soient mis en place pour protéger la vie privée. L'OSSNR aura le pouvoir d'examiner tous les types d'ensembles de données assujettis au régime. Le CPSNR fournira un mécanisme de responsabilisation supplémentaire dans le cadre de son mandat continu d'examiner les activités de sécurité nationale du Canada.

Service canadien du renseignement de sécurité (SCRS)

A1.8 Le rôle principal du SCRS est de faire enquête sur les activités soupçonnées de constituer des menaces pour la sécurité du Canada (au sens de l'article 2 de la *Loi sur le SCRS*) et de faire rapport sur ces activités au gouvernement du Canada. Le SCRS peut également prendre des mesures pour réduire la menace. Ses activités doivent être exécutées conformément à la *Loi sur le SCRS*, qui prévoit des exigences en matière de collecte, de conservation et de communication de renseignements. Le SCRS doit également mener ses activités conformément à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*, entre autres lois, ainsi qu'à l'Instruction ministérielle et aux politiques et procédures internes. Toute activité opérationnelle nécessite une autorisation, même si elle n'exige pas d'autorisation judiciaire en vertu de l'article 21 de la *Loi sur le SCRS*. L'Instruction ministérielle donne des directives au SCRS selon lesquelles plus le risque associé à une activité particulière est élevé, plus l'autorité requise pour l'approbation est élevée. Elle fournit également des indications selon lesquelles le Service doit employer les techniques opérationnelles les moins intrusives proportionnelles à la menace.

A1.9 En ce qui a trait à la capacité actuelle du Comité de surveillance des activités de renseignement de sécurité (CSARS) de remédier au non-respect de la *Loi sur le SCRS* et à l'Instruction ministérielle, le Comité a le pouvoir de formuler des constatations et des recommandations non contraignantes. Celles-ci sont envoyées au ministre de la Sécurité publique et de la Protection civile dans le cadre de rapports classifiés. Les versions non classifiées sont publiées dans un rapport public une fois par an, ce qui assure la transparence et l'examen public des activités du SCRS. En ce qui concerne le processus de plainte du CSARS, un particulier peut déposer une plainte auprès du Comité conformément à la *Loi sur le SCRS*. Toute personne, y compris les non-Canadiens, peut déposer une plainte auprès du CSARS. Le processus de plainte est le même, indépendamment de la nationalité, à l'exception du fait que les non-Canadiens à l'extérieur du Canada ne peuvent pas bénéficier de la protection de la *Charte canadienne des droits et libertés*. Les rapports de plaintes peuvent également contenir des recommandations non contraignantes. De plus, le Commissaire fédéral à la protection de la vie privée a accès, lorsqu'il enquête

sur une plainte concernant les activités du SCRS, à toutes les informations, à l'exception des documents confidentiels du Cabinet.

Accès aux données à des fins de sécurité nationale

A1.10 Les données sur les personnes de l'UE stockées au Canada ne seraient accessibles que si elles étaient pertinentes pour une enquête policière canadienne ou une enquête du SCRS, par exemple si une personne de l'UE était soupçonnée d'avoir commis un crime au Canada. Cet accès serait fondé sur le respect des autorités juridiques applicables et les restrictions régissant l'accès licite aux données, y compris l'obligation d'autorisation judiciaire, selon les données recherchées. Séparément, le CST a pour mandat d'acquiescer et d'utiliser des renseignements aux fins de fournir du renseignement étranger, conformément aux priorités du gouvernement du Canada en matière de renseignement. Dans le cadre de son mandat d'assistance, le CST peut fournir de l'aide à la GRC et au SCRS au cours d'une enquête pour aider à résoudre les problèmes techniques d'accès aux preuves numériques ou aux renseignements qui ont été obtenus légalement. Cela doit être fait en conformité avec toutes les autorités juridiques pertinentes et les restrictions régissant l'accès licite aux données, y compris les autorisations judiciaires.

Modifications à la LPRPDE en 2004 en conséquence de la Loi sur la sécurité publique, 2002

A1.11 La jurisprudence suivante donne des exemples de décisions où le [traduction] « critère de soupçons raisonnables » a été appliqué. Toutefois, il n'y a aucune jurisprudence pertinente où ce critère a été appliqué ou discuté en relation avec la LPRPDE.

- *R. c. Mahmood*, [2008] O.J. N° 3922¹⁹
- *R. c. Merritt*, [2017] ONSC 366²⁰
- *Ontario c. Bharath*, 2016 ONCJ 382²¹
- *R. c. Chehil*, 2008 NSSC 357²²
- *Stevens c. SNF Maritime Metal Inc.*, 2010 CF 1137²³
- *R. c. Devloo*, [2015] ABQB 345²⁴

Accès aux renseignements personnels par des ressortissants étrangers

A1.12 La *Loi sur la protection des renseignements personnels* n'accorde pas aux citoyens étrangers qui ne sont pas présents au Canada le droit de faire une demande d'accès pour leurs renseignements

¹⁹https://www.canlii.org/en/on/onsc/doc/2008/2008canlii51774/2008canlii51774.html?autocompleteStr=R%20v.%20mahmood&autocompletePos=3#_Toc211144885 (en anglais seulement)

²⁰<https://www.canlii.org/en/on/onsc/doc/2017/2017onsc366/2017onsc366.html?autocompleteStr=R.%20v.%20Merritt%2C%202017%20ONSC%20366&autocompletePos=1> (en anglais seulement)

²¹<https://www.canlii.org/en/on/oncj/doc/2016/2016oncj382/2016oncj382.html?autocompleteStr=Ontario%20v.%20Bharath%2C%202016%20ONCJ%20382&autocompletePos=1> (en anglais seulement)

²²<https://www.canlii.org/en/ns/nssc/doc/2008/2008nssc357/2008nssc357.html?autocompleteStr=%09R.%20v.%20Chehil%202008%20NSSC%20357&autocompletePos=1> (en anglais seulement)

²³ <https://www.canlii.org/fr/ca/cfpi/doc/2010/2010cf1137/2010cf1137.html>

²⁴<https://www.canlii.org/en/ab/abqb/doc/2015/2015abqb345/2015abqb345.html?autocompleteStr=R.%20v.%20Devloo%20&autocompletePos=1> (en anglais seulement)

personnels relevant des institutions fédérales²⁵. Par conséquent, la *Loi sur la protection des renseignements personnels* n'offre pas non plus à ces personnes de droits liés au droit de demander l'accès à leurs renseignements personnels, y compris le droit de demander une correction, d'exiger qu'une notation soit faite reflétant une demande de correction refusée et d'exiger que l'on notifie de la correction ou de la notation toute personne ou tout organisme à qui les renseignements ont été communiqués.

A1.13 Toutefois, les citoyens étrangers sont en mesure d'accéder à leurs renseignements personnels par l'entremise de la *Loi sur l'accès à l'information*. La *Loi sur l'accès à l'information* offre un droit d'accès aux renseignements détenus par le gouvernement aux citoyens canadiens, aux résidents permanents et aux personnes et sociétés présentes au Canada. En outre, toute personne à l'extérieur du Canada peut faire une demande d'accès par l'entremise d'un mandataire canadien. La *Loi sur l'accès à l'information* interdit la communication d'un document demandé en vertu de cette loi s'il contient des renseignements personnels; toutefois, un tel document peut être communiqué si, entre autres choses, la personne à laquelle il se rapporte consent à ce qu'il le soit. Par conséquent, dans de tels cas, un mandataire situé au Canada et agissant pour le compte d'un ressortissant étranger pourrait présenter une demande de documents divers en vertu de la LAI concernant le ressortissant étranger, qui, à son tour, pourrait consentir à la communication de ses renseignements personnels au mandataire.

Les ressortissants étrangers bénéficient du Code de pratiques équitables en matière de renseignements

A1.14 Les citoyens étrangers qui ne sont pas présents au Canada bénéficient de protections fixées par le Code de pratiques équitables en matière de renseignements consacrées aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*. Ces dispositions établissent les exigences relatives à la collecte (articles 4 et 5), à l'utilisation (article 7), à la communication (article 8) et à la conservation et l'élimination (article 6) des renseignements personnels. Ces dispositions portent principalement sur la gestion des renseignements personnels par les institutions gouvernementales. Elles ne tiennent pas compte de la base du statut de citoyenneté ou de l'emplacement géographique de la personne à qui les renseignements personnels se rapportent et ne font pas de distinction à cet effet. Les exigences fixées par les articles 4 à 8 sont contraignantes pour les institutions gouvernementales.

Surveillance par le commissaire à la protection de la vie privée du Canada et la Cour fédérale

A1.15 Comme les ressortissants étrangers n'ont pas le droit de demander l'accès à leurs renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*, ils ne peuvent déposer une plainte auprès du commissaire à la protection de la vie privée du Canada lorsqu'une institution du gouvernement fédéral leur refuse l'accès à leurs renseignements personnels. Toutefois, le traitement (c.-à-d. la collecte, l'utilisation, la communication, la conservation et l'élimination) inapproprié de renseignements personnels par une institution gouvernementale permet à la personne à qui les renseignements personnels se rapportent de déposer une plainte auprès du commissaire à la protection de la vie privée du Canada²⁶, y compris les citoyens étrangers qui ne sont

²⁵ *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21.

²⁶ *Ibid.*, alinéas 29(1)a) et h).

pas présents au Canada. Si une enquête du commissaire à la protection de la vie privée du Canada révèle qu'une plainte est fondée, le commissaire peut formuler un rapport contenant des recommandations aux institutions gouvernementales et demander à celles-ci qu'elles l'informent dans un délai déterminé « soit des mesures prises ou envisagées pour la mise en œuvre de ses recommandations, soit des motifs invoqués pour ne pas y donner suite »²⁷.

A1.16 Un traitement inapproprié des renseignements personnels par les institutions gouvernementales permet également à « quiconque est directement touché » de faire une demande de contrôle judiciaire en vertu de la *Loi sur les Cours fédérales*²⁸. Cela inclut les citoyens étrangers qui ne sont pas présents au Canada. La *Loi sur les Cours fédérales* permet à la Cour fédérale d'« ordonner à l'office fédéral en cause d'accomplir tout acte qu'il a illégalement omis ou refusé d'accomplir ou dont il a retardé l'exécution de manière déraisonnable »²⁹. La Loi permet également à la Cour fédérale de « déclarer nul ou illégal, ou annuler, ou infirmer et renvoyer pour jugement conformément aux instructions qu'elle estime appropriées, ou prohiber ou encore restreindre toute décision, ordonnance, procédure ou tout autre acte de l'office fédéral »³⁰. La *Loi sur les Cours fédérales* donne au terme « office fédéral » la définition « conseil, bureau, commission ou autre organisme, ou personne ou groupe de personnes, ayant, exerçant ou censé exercer une compétence ou des pouvoirs prévus par une loi fédérale ou par une ordonnance prise en vertu d'une prérogative royale », avec des exceptions³¹. Il existe des précédents pour demander à la Cour fédérale d'examiner les mesures relatives aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels* en vertu de la *Loi sur les Cours fédérales*³².

²⁷ *Loi sur la protection des renseignements personnels*, paragraphe 35(1).

²⁸ *Loi sur les Cours fédérales*, paragraphe 18.1(1).

²⁹ *Ibid.*, alinéa 18.1(3)a).

³⁰ *Ibid.*, alinéa 18.1(3)b).

³¹ *Ibid.*, paragraphe 2(1). Les exceptions se rapportent à la Cour canadienne de l'impôt et à ses juges ainsi qu'aux organismes et juges provinciaux. Pour de plus amples renseignements sur le terme « office fédéral », voir le paragraphe 29 de l'affaire *Anisman c. Canada (Agence des services frontaliers)*, 2010 CAF 52.

³² Voir *Sauvé c. Canada (Procureur général)*, 2016 CF 401, *Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN) c. Canada (Procureur général)*, 2016 CF 1289 et *Kelly A. O'Grady c. Procureur général du Canada*, 2017 CF 167.