BIBLIOTHÈQUE DU PARLEMENT
LIBRARY OF PARLIAMENT

RÉSUMÉ LÉGISLATIF

PROJET DE LOI C-59 : LOI CONCERNANT DES QUESTIONS DE SÉCURITÉ NATIONALE

Publication nº 42-1-C59-F
Le 3 juin 2019

Tanya Dupuis
Chloé Forget
Holly Porteous
Dominique Valiquet
Division des affaires juridiques et sociales
Service d'information et de recherche parlementaires

Les ***résumés législatifs*** de la Bibliothèque du Parlement résument des projets de loi étudiés par le Parlement et en exposent le contexte de façon objective et impartiale. Ils sont préparés par le Service d'information et de recherche parlementaires, qui effectue des recherches et prépare des informations et des analyses pour les parlementaires, les comités du Sénat et de la Chambre des communes et les associations parlementaires. Les résumés législatifs sont mis à jour au besoin pour tenir compte des amendements apportés aux projets de loi au cours du processus législatif.

Avertissement : Par souci de clarté, les propositions législatives du projet de loi décrit dans le présent résumé législatif sont énoncées comme si elles avaient déjà été adoptées ou étaient déjà en vigueur. Il ne faut pas oublier, cependant, qu'un projet de loi peut faire l'objet d'amendements au cours de son examen par la Chambre des communes et le Sénat, et qu'il est sans effet avant d'avoir été adopté par les deux Chambres du Parlement, d'avoir reçu la sanction royale et d'être entré en vigueur.

Dans ce document, tout changement d'importance depuis la dernière publication est signalé en **caractères gras**.

Résumé législatif du projet de loi C-59
(Résumé législatif)

Publication nº 42-1-C59-F

This publication is also available in English.

TABLE DES MATIÈRES

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-59 : LOI CONCERNANT DES QUESTIONS DE SÉCURITÉ NATIONALE

1 CONTEXTE

Le 20 juin 2017, le ministre de la Sécurité publique et de la Protection civile a déposé à la Chambre des communes le projet de loi C-59, Loi concernant des questions de sécurité nationale (titre abrégé : « Loi de 2017 sur la sécurité nationale ») [1].

Le projet de loi C-59 est l'aboutissement d'une longue série d'événements, de commissions d'enquête, de consultations publiques et de mesures législatives concernant le terrorisme et la sécurité nationale, dont voici les principaux, en ordre chronologique :

- 1977-1981 : Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Commission McDonald) [2];
- 1984 : En réponse aux recommandations de la Commission McDonald, création d'un service de renseignement civil (le Service canadien du renseignement de sécurité ou SCRS) en remplacement du Service de sécurité nationale de la Gendarmerie royale du Canada;
- 1985 : Attentat à la bombe commis contre le vol 182 d'Air India;
- 2001 : *Loi antiterroriste* adoptée à la suite des attentats du 11 septembre aux États-Unis;
- 2006 : Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar (Commission O'Connor) [3];
- 2008 : Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin (commission Iacobbuci) [4];
- 2010 : Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India (commission Major) [5];
- 2014 : Attentats terroristes à Ottawa et à Saint-Jean-sur-Richelieu, au Québec;
- 2015 : Adoption de la *Loi antiterroriste de 2015* (projet de loi C-51) [6];
- 2016 : Consultations du gouvernement – *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016* [7];
- 2017 : Rapport sur les consultations – *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris* [8];
- 2017 : Adoption de la *Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement* (projet de loi C- 22) [9].

1.1 OBJET ET PRINCIPALES MODIFICATIONS DU PROJET DE LOI C-59

Le projet de loi C-59 peut être considéré comme une mesure législative « majeure » en matière de sécurité nationale, et ce, pour au moins deux raisons :

- il crée un système global d'examen des activités de sécurité nationale (par opposition au système fragmentaire actuel) faisant contrepoids tant aux pouvoirs des organismes du renseignement qu'à l'application de la *Loi antiterroriste*, qui a été élargie depuis 2001;
- il amende certains aspects de l'ancien projet de loi C-51 (*Loi antiterroriste de 2015)*, considérés par certains comme contraires à la *Charte canadienne des droits et libertés* [10].

Le projet de loi C-59 est divisé en 11 parties :

- Les parties 1 et 2 du projet de loi créent deux nouvelles institutions fédérales responsables de l'examen des activités de sécurité nationale, respectivement l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (art. 2 à 49) et le commissaire au renseignement (art. 50 à 75).
- La partie 1.1 du projet de loi édicte la Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (art. 49.1 et 49.2).
- Les parties 3 et 4 du projet de loi portent sur deux des principaux organismes chargés du renseignement, respectivement le Centre de la sécurité des télécommunications et le Service canadien du renseignement de sécurité (art. 76 à 111).
- Les parties 5 et 6 du projet de loi visent à mieux encadrer les régimes d'échange de renseignements utilisés, respectivement, entre les institutions fédérales et par les personnes chargées de la gestion de la liste « d'interdiction de vol », prévus dans la *Loi antiterroriste de 2015* (art. 112 à 139).
- Les parties 7 et 8 du projet de loi sont conçues respectivement pour resserrer les règles spéciales en matière de prévention d'activités terroristes et pour veiller à ce que les adolescents soupçonnés bénéficient de protections adéquates (art. 140 à 167).
- La partie 9 du projet de loi (art. 168) prévoit un examen parlementaire du projet de loi C-59 après cinq ans – si possible en parallèle avec l'examen de la *Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement*.
- La partie 10 du projet de loi (art. 169 à 173) prévoit l'entrée en vigueur du projet de loi C-59.

2 DESCRIPTION ET ANALYSE

2.1 PARTIE 1 : ÉDICTION DE LA LOI SUR L'OFFICE DE SURVEILLANCE DES ACTIVITÉS EN MATIÈRE DE SÉCURITÉ NATIONALE ET DE RENSEIGNEMENT (ART. 2 À 49)

La partie 1 du projet de loi édicte la Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (titre abrégé : « Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement » [Loi sur l'OSASNR]) afin de créer l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSASNR), dont le modèle reprend à peu près celui du Comité de surveillance des activités de renseignement de sécurité (CSARS), l'organe actuellement chargé de contrôler la légalité des activités du SCRS.

L'article 3 de la Loi sur l'OSASNR prévoit la nomination d'au moins quatre et d'au plus sept membres de l'OSASNR, dont son président. L'article 4 de la Loi sur l'OSASNR dispose que les membres de l'OSASNR seront nommés par le gouverneur en conseil pour un mandat de cinq ans, que leur mandat pourra être renouvelé pour une période maximale de cinq ans et qu'ils ne peuvent être démis que pour un motif valable. Le paragraphe 4(7) de la Loi sur l'OSASNR précise que, selon leur désignation, le président et le vice-président peuvent exercer leur charge à temps plein ou à temps partiel.

Les paragraphes 6(1) et 6(2) de la Loi sur l'OSASNR indiquent que le gouverneur en conseil doit agir en accord avec les directives du Conseil du Trésor en ce qui concerne l'établissement de la rémunération et des frais.

Les articles 49 et 50 de la Loi sur l'OSASNR exigent respectivement des membres de l'OSASNR qu'ils prêtent serment ou fassent une déclaration solennelle et conservent l'habilitation de sécurité du gouvernement du Canada. Les modifications proposées à la *Loi sur la protection de l'information* (LPI)[11], à l'article 35 du projet de loi, donnent à penser que les membres actuels et anciens de l'OSASNR seront tenus au secret à perpétuité, au sens de la LPI, ce qui sous-entend qu'eux-mêmes et les employés du Secrétariat de l'OSASNR auront connaissance de renseignements opérationnels spéciaux sur les sources et les méthodes en matière de sécurité et de renseignement.

Les articles 41 à 48 de la Loi sur l'OSASNR renferment les dispositions relatives à la constitution d'un secrétariat pour soutenir les travaux de l'OSASNR.

2.1.1 Mandat de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement

Le mandat que l'article 8 de la Loi sur l'OSASNR confère à l'OSASNR est vaste, étant donné que l'OSASNR est investi du pouvoir de procéder à un examen et de formuler des conclusions et des recommandations, non seulement sur la légalité, mais aussi sur le caractère raisonnable et la nécessité de toutes les activités liées à la sécurité nationale ou au renseignement exercées par le SCRS, le Centre de la sécurité des télécommunications (CST) et les ministères fédéraux, ou confiées à l'OSASNR par un ministre. Le paragraphe 8(3) de la Loi sur l'OSASNR précise que l'OSASNR peut formuler des conclusions et des recommandations sur la conformité à la loi et à toute directive ministérielle applicable, ainsi que sur le caractère raisonnable et la nécessité de l'exercice des pouvoirs d'un ministère.

Afin de préciser la portée du mandat de l'OSASNR, l'article 7.1 de la Loi sur l'OSASNR dispose que l'OSASNR peut déterminer la procédure à suivre dans l'exercice de ses attributions.

Comme le soulignent les dispositions transitoires énoncées aux articles 3 à 17 du projet de loi, l'OSASNR abolit le CSARS et le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST); ce dernier étant chargé actuellement de l'examen de la légalité des activités du CST.

2.1.2 Régime d'accès à l'information à deux volets

L'article 11 de la Loi sur l'OSASNR précise qu'aux fins de l'examen et des enquêtes sur les plaintes, l'OSASNR est en droit de recevoir de l'administrateur général et des employés du ministère en cause « les documents et explications dont il estime avoir besoin dans l'exercice de ses attributions ».

Parallèlement, le projet de loi C-59 crée deux régimes d'accès à l'information distincts pour l'OSASNR; l'un pour ses travaux d'examen et l'autre pour ses enquêtes sur les plaintes.

2.1.2.1 Examens

Le paragraphe 8(2.1) de la Loi sur l'OSASNR exige de l'OSASNR qu'il examine la mise en œuvre des aspects importants des instructions et directives ministérielles, nouvelles ou modifiées, qui sont données au SCRS, au CST ou à tout autre ministère, si elles concernent la sécurité nationale ou le renseignement.

L'article 9 de la Loi sur l'OSASNR porte sur l'accès à l'information relativement au travail d'examen de l'OSASNR. Exception faite des renseignements confidentiels du Cabinet, l'OSASNR aura, en temps opportun, un accès général à l'information, y compris l'information protégée par le secret professionnel de l'avocat ou du notaire ou

par le privilège relatif au litige. En précisant qu'il peut s'agir d'information « en la possession de tout ministère », le paragraphe 9(1) de la Loi sur l'OSASNR donne à l'OSASNR un droit d'accès à l'information et au renseignement provenant de tiers, comme le renseignement communiqué par des pays alliés [12].

Il convient de souligner que les pouvoirs que l'on propose de donner à l'OSASNR relativement à ses fonctions d'examen sont plus restreints que ceux du commissaire du CST qui, en vertu du paragraphe 273.63(4) de la *Loi sur la défense nationale* [13], disposait de tous les pouvoirs d'un commissaire au sens de la partie II de la *Loi sur les enquêtes* [14] pour s'acquitter de ses fonctions. Cette diminution de pouvoirs a des répercussions sur les conditions en vertu desquelles l'OSASNR aura accès à l'information.

Tandis que le CSARS et le BCCST rendaient compte respectivement des conclusions de leur examen au ministre de la Sécurité publique et de la Protection civile et au ministre de la Défense nationale, l'OSASNR relève d'un « ministre fédéral » responsable de l'OSASNR, tel que le gouverneur en conseil l'aura désigné en vertu de l'article 55 de la Loi sur l'OSASNR.

2.1.2.2 Enquêtes

Aux termes de l'article 8 de la Loi sur l'OSASNR, l'OSASNR prendra en charge les responsabilités du CSARS et du BCCST à l'égard des enquêtes sur les plaintes visant les activités du SCRS et du CST, notamment les plaintes de dénonciateurs comportant des renseignements opérationnels spéciaux et les plaintes concernant des avis donnés par le SCRS à des administrateurs généraux sur des autorisations de sécurité individuelles et des évaluations de la menace relatives à des demandes de citoyenneté. L'OSASNR prendra aussi en charge les plaintes visant les activités de sécurité nationale de la Gendarmerie royale du Canada (GRC). La distinction entre les plaintes devant faire l'objet d'une enquête de la Commission civile d'examen et de traitement des plaintes relatives à la GRC et celles devant faire l'objet d'une enquête de l'OSASNR sera établie au moyen de modifications à la *Loi sur la Gendarmerie royale du Canada* [15], conformément aux articles 41 à 43 du projet de loi C-59.

L'article 10 de la Loi sur l'OSASNR crée un régime d'accès à l'information distinct pour l'OSASNR en ce qui concerne son rôle d'enquête sur les plaintes. L'article 27 de la Loi sur l'OSASNR habilite l'OSASNR à contraindre des témoins à comparaître devant lui pour déposer verbalement ou par écrit sous serment, et à « recevoir des éléments de preuve ou des informations par déclaration verbale ou écrite sous serment ou par tout autre moyen qu'il estime indiqué, indépendamment de leur admissibilité devant les tribunaux ».

Il convient de souligner que l'article 10 de la Loi sur l'OSASNR limite le droit d'accès de l'OSASNR aux informations qui sont en la possession ou sous le contrôle de trois organismes seulement : le SCRS, le CST et la GRC.

En ce qui concerne les enquêtes ministérielles, l'article 7 de la *Loi sur les enquêtes* autorise les commissaires à « visiter tout bureau ou établissement public, avec droit d'accès dans tous les locaux »; à « examiner tous papiers, documents, pièces justificatives, archives et registres appartenant à ce bureau ou établissement »; et à assigner des témoins et les contraindre à déposer oralement ou par écrit sous la foi du serment ou d'une affirmation solennelle. L'article 8 de la *Loi sur les enquêtes* autorise les commissaires à assigner des témoins à comparaître pour témoigner et produire des documents.

Pour éviter tout double emploi, le paragraphe 15.1(1) de la Loi sur l'OSASNR permet à l'OSASNR de coordonner ses activités avec celles que mène le commissaire à la protection de la vie privée en vertu du paragraphe 37(1) de la *Loi sur la protection des renseignements personnels*[16] (LPRP). Aux fins de la coordination, l'OSASNR peut également communiquer au commissaire à la protection de la vie privée des renseignements liés aux examens que mène l'OSASNR en vertu de l'article 8 de la Loi sur l'OSASNR.

L'article 27.1 de la Loi sur l'OSASNR oblige l'OSASNR à suspendre une enquête s'il estime, après avoir consulté le ministère concerné, que la poursuivre serait de nature à compromettre une enquête ou une procédure en matière pénale en cours, ou y nuirait sérieusement.

Le paragraphe 52(1) de la Loi sur l'OSASNR précise qu'afin d'éviter la communication de renseignements confidentiels, l'OSASNR doit consulter les administrateurs généraux concernés pour produire les résumés aux plaignants ou les rapports sur les autorisations de sécurité ou les demandes de citoyenneté rejetées. La façon dont seront gérés d'éventuels différends sur le caviardage des documents en question ou des rapports publics annuels de l'OSASNR n'est pas précisée.

L'article 46 du projet de loi modifie l'article 53 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*[17] de façon à ajouter le nouvel article 53.4 pour préciser que la communication d'information provenant du Centre d'analyse des opérations et déclarations financières du Canada (le Centre) destinées à l'OSASNR se fera par l'entremise du ministre des Finances et non pas directement par le directeur du Centre. Cette disposition vise essentiellement à éviter des contacts directs entre le Centre et l'OSASNR.

2.1.3 Rapports annuels

Aux termes du paragraphe 38(1) de la Loi sur l'OSASNR, le premier ministre recevra un rapport annuel portant sur les activités de l'OSASNR pour l'année civile précédente, ainsi que sur les conclusions et recommandations que l'OSASNR aura formulées durant la même période. Un exemplaire du rapport doit être déposé au Sénat et à la Chambre des communes dans les 15 jours de séance suivant la présentation dudit rapport au premier ministre.

L'article 39 de la Loi sur l'OSASNR exige que l'OSASNR présente au ministre de la Sécurité publique et de la Protection civile un rapport portant sur l'information communiquée sous le régime de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*[18] modifiée.

En vertu de l'article 40 de la Loi sur l'OSASNR, lorsque l'OSASNR produit un rapport spécial dont il estime qu'il est d'intérêt public, le rapport doit être présenté au ministre compétent.

Dans les deux cas, le ministre de la Sécurité publique et de la Protection civile est tenu de déposer un exemplaire du rapport devant le Sénat et la Chambre des communes dans les 15 jours de séance suivant sa réception.

Certaines exigences auxquelles doit se soumettre actuellement le CSARS en matière de production de rapports ne seront pas imposées à l'OSASNR. Par exemple, le régime actuel exige que le rapport annuel du CSARS précise le nombre de mandats délivrés au cours de l'exercice aux termes de l'article 21.1 de la *Loi sur le Service canadien du renseignement de sécurité*[19] (Loi sur le SCRS), ainsi que le nombre de demandes de mandats présentées en vertu de cet article qui ont été refusées dans la même période. Le projet de loi C-59 n'établit aucune exigence de ce genre en matière de production de rapports.

2.1.4 Secrétariat

L'article 41 de la Loi sur l'OSASNR établit le Secrétariat de l'OSASNR pour aider l'OSASNR à s'acquitter de son mandat.

Comme le prévoit l'article 42 de la Loi sur l'OSASNR, le directeur général du Secrétariat de l'OSASNR est nommé par le gouverneur en conseil pour un mandat renouvelable d'au plus cinq ans. Les articles 45 et 46 de la Loi sur l'OSASNR décrivent les pouvoirs du directeur général, qui, en vertu de l'article 42, a rang d'administrateur général de ministère, en matière de nomination et de licenciement du personnel. Ces pouvoirs correspondent à ceux du chef du CST, définis à l'article 13 de la Loi sur le Centre de la sécurité des télécommunications (Loi sur le CST, édictée par l'article 76 du projet de loi C-59).

Aux termes de l'article 30 du projet de loi C-59, le Secrétariat de l'OSASNR est désigné comme étant un organisme distinct en application de l'annexe V de la *Loi sur la gestion des finances publiques*[20] (LGFP), ce qui signifie qu'il fait partie de la fonction publique et qu'il est assujetti à la *Loi sur l'emploi dans la fonction publique*[21] (LEFP). Selon le paragraphe 35(1) de la LEFP, pour le personnel des organismes distincts, sauf interdiction explicite, la mobilité entre les organismes distincts et les autres organismes de la fonction publique est ouverte dans les deux sens. Par exemple, des employés d'organismes de sécurité nationale ou de renseignement pourraient être détachés au Secrétariat de l'OSASNR, puis retourner à leur poste d'attache par la suite.

2.2 PARTIE 1.1 : LOI VISANT À ÉVITER LA COMPLICITÉ DANS LES CAS DE MAUVAIS TRAITEMENTS INFLIGÉS PAR DES ENTITÉS ÉTRANGÈRES (ART. 49.1 ET 49.2)

La partie 1.1 du projet de loi C-59 édicte la Loi concernant la communication et la demande de renseignements qui entraîneraient un risque sérieux que de mauvais traitements soient infligés à un individu par une entité étrangère et l'utilisation de renseignements vraisemblablement obtenus par suite de tels traitements (titre abrégé : « Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères » [LECCMTIET]). Aux termes de l'article 3 de la LECCMTIET, le gouverneur en conseil a le pouvoir de donner des instructions concernant la communication, la demande et l'utilisation de renseignements qui risqueraient fortement d'exposer une personne à de mauvais traitements. En vertu de la LECCMTIET, le gouverneur en conseil est tenu de donner ces instructions au chef d'état-major de la Défense, au sous-ministre de la Défense nationale, au sous-ministre des Affaires étrangères, au commissaire de la GRC, au directeur du SCRS, au président de l'Agence des services frontaliers du Canada (ASFC) et au chef du CST. Les articles 5 et 6 de la LECCMTIET disposent respectivement que, dès que possible après avoir reçu ces instructions, les administrateurs généraux doivent les rendre publiques et en transmettre une copie au Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et, le cas échéant, à l'organisme d'examen concerné.

Le paragraphe 3(3) de la LECCMTIET précise que les instructions données en application de cette loi ne constituent pas des textes réglementaires.

Selon l'article 7 de la LECCMTIET, l'administrateur général à qui de telles instructions ont été données doit soumettre au ministre compétent, avant le 1er mars de chaque année, un rapport sur la mise en œuvre de ces instructions et, dès que possible, en mettre une version caviardée à la disposition du public. Aux termes de l'article 8 de la LECCMTIET, le ministre compétent doit remettre une copie du rapport au CPSNR et à l'OSASNR et, le cas échéant, à la Commission civile d'examen et de traitement des plaintes relatives à la GRC.

2.3 PARTIE 2 : ÉDICTION DE LA LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT (ART. 50 À 75)

L'article 50 du projet de loi édicte la Loi concernant le bureau du commissaire au renseignement (titre abrégé : « Loi sur le commissaire au renseignement » [LCR]), laquelle crée le Bureau du commissaire au renseignement. Aux termes de l'article 12 de la LCR, les attributions du commissaire consistent à assurer la surveillance d'un sous-groupe d'activités du CST et du SCRS. Le Bureau du commissaire au renseignement remplace le Bureau du commissaire du CST.

L'article 4 de la LCR précise que le commissaire au renseignement doit être un juge à la retraite d'une juridiction supérieure [22]. Selon les paragraphes 4(1) et 4(2) de la LCR, le commissaire au renseignement sera nommé à titre inamovible pour un mandat maximal de cinq ans renouvelable une seule fois.

L'Énoncé concernant la *Charte* du ministère de la Justice dit que la LCR :

> créerait un poste indépendant et quasi-judiciaire de commissaire au renseignement, chargé d'évaluer et d'examiner certaines décisions ministérielles concernant les activités en matière de collecte de renseignements et de cybersécurité. Cela assurerait un examen indépendant de la protection de la vie privée et des autres intérêts visés par ces activités d'une manière dûment adaptée au contexte délicat de la sécurité nationale [23].

Le projet de loi ne précise ni la tribune ni la norme qui seraient utilisées à l'égard de ces décisions [24].

Le paragraphe 6(3) de la LCR dispose que, pour l'application de la partie 7 de la LEFP, laquelle porte sur les activités politiques des employés, le commissaire au renseignement est réputé être un administrateur général, c'est-à-dire qu'il lui est interdit de participer à toute activité politique autre que l'exercice de son droit de vote dans le cadre d'une élection.

À l'instar du directeur général du Secrétariat de l'OSASNR, le commissaire au renseignement jouit d'un pouvoir discrétionnaire considérable en ce qui concerne l'embauche et le licenciement du personnel. Le libellé utilisé au paragraphe 6(3) de la LCR pour décrire les pouvoirs du commissaire au renseignement à cet égard reprend presque mot pour mot celui utilisé pour décrire les pouvoirs du chef du CST à l'article 13 de la Loi sur le CST (édictée à l'article 76 du projet de loi C-59).

Comme dans le cas du Secrétariat de l'OSASNR, l'article 65 du projet de loi C-59 ajoute le Bureau du commissaire au renseignement à la liste des organismes distincts de l'annexe V de la LGFP, de sorte que le Bureau fait partie de la fonction publique et qu'il est assujetti à la LEFP. Ainsi, en vertu du paragraphe 35(1) de la LEFP, des employés d'organismes de sécurité nationale ou de renseignement pourraient être détachés au Bureau du commissaire au renseignement.

Les articles 51 à 59 du projet de loi C-59 prévoient le transfert des ressources du Bureau du commissaire du CST au Bureau du commissaire au renseignement.

2.3.1 Examens du commissaire au renseignement

2.3.1.1 Pouvoirs

Selon l'article 12 de la LCR, le commissaire au renseignement est chargé :

> a) d'examiner les conclusions sur lesquelles reposent certaines autorisations accordées ou modifiées et certaines déterminations effectuées au titre de la *Loi sur le Centre de la sécurité des télécommunications* et de la *Loi sur le Service canadien du renseignement de sécurité*;
>
> b) d'approuver, si ces conclusions sont raisonnables, ces autorisations, modifications et déterminations.

Comme l'indiquent les articles 13 et 14 de la LCR, les « certaines autorisations » mentionnées à l'article 12 de la LCR sont délivrées principalement par le ministre responsable du CST (actuellement, le ministre de la Défense nationale)[25] sur demande écrite du chef du CST, et elles se rapportent aux activités de collecte de renseignements étrangers et de cybersécurité du CST[26]. Plus précisément, lorsque le CST propose de mener des activités de collecte de renseignements étrangers ou de cybersécurité qui risquent de contrevenir à une loi fédérale, il doit demander une autorisation ministérielle, et le commissaire au renseignement doit approuver cette autorisation[27]. Aux termes des articles 15 et 18 de la LCR respectivement, le commissaire doit aussi examiner le caractère raisonnable des modifications desdites autorisations ainsi que les conclusions sur lesquelles s'appuie toute autorisation délivrée par le directeur du SCRS pour permettre l'interrogation d'un ensemble de données en situation d'urgence. Comme l'établit l'article 110 du projet de loi C-59, dans la Loi sur le SCRS modifiée, un ensemble de données s'entend d'un « ensemble d'informations sauvegardées sous la forme d'un fichier numérique qui portent sur un sujet commun ».

Le terme « déterminations », à l'article 12 de la LCR, renvoie aux décisions prises par le ministre de la Sécurité publique et de la Protection civile d'autoriser le SCRS à recueillir des ensembles de données canadiens ou à conserver des ensembles de données étrangers, comme le prévoient les articles 16 et 17 de la LCR. Le ministre fera aussi des déterminations concernant la justification en droit du SCRS de commettre des catégories d'actes ou d'omissions qui constitueraient autrement des infractions. Plus précisément, les déterminations du ministre fourniraient aux employés désignés du SCRS les fondements juridiques les autorisant à commettre ou à ordonner que soient commis des actes ou des omissions qui constitueraient autrement des infractions, afin de permettre au SCRS de s'acquitter de son mandat de collecte d'informations et de renseignements et de réduction de la menace (art. 19 de la LCR et nouvel art. 20.1 de la Loi sur le SCRS, édictés par l'art. 101 du projet de loi).

En vertu du paragraphe 23(1) et de l'article 26 de la LCR, exception faite des documents confidentiels du Cabinet, le commissaire au renseignement aura un droit d'accès à tous les renseignements dont la personne disposait pour prendre la décision que le commissaire examine, y compris les renseignements protégés par le secret professionnel de l'avocat. L'article 25 de la LCR dispose que les ministres responsables du SCRS et du CST, ainsi que le SCRS et le CST directement, peuvent communiquer d'autres renseignements au commissaire. En outre, l'article 75 du projet de loi, qui modifie l'article 24 de la LCR, autorise le commissaire au renseignement à recevoir des rapports du CPSNR et de l'OSASNR.

2.3.1.2 Décisions

L'article 20 de la LCR exige que toutes les décisions du commissaire au renseignement soient présentées par écrit. En ce qui concerne les autorisations nouvelles et modifiées aux fins des activités de collecte de renseignements étrangers et de cybersécurité, les déterminations faites par le directeur du SCRS relativement à des ensembles de données canadiens ainsi que les autorisations données par le directeur du SCRS concernant l'interrogation d'ensembles de données en situation d'urgence, le commissaire a deux options : approuver ou ne pas approuver l'autorisation et la détermination en question. Lorsqu'il examine les conclusions qui ont formé le fondement de décisions de conserver des ensembles de données étrangers, le commissaire au renseignement a trois options : approuver, approuver sous réserve de conditions ou refuser d'approuver l'autorisation. Toutes les décisions doivent être motivées.

La plupart des décisions du commissaire au renseignement doivent être prises dans les 30 jours suivant la date de réception d'un avis de l'autorisation, mais, aux termes de l'alinéa 20(3)b) de la LCR, le CST et le SCRS peuvent tenter de négocier un délai plus court. Lorsque le directeur du SCRS a délivré une autorisation aux fins de l'interrogation d'un ensemble de données canadien ou étranger en situation

d'urgence, le commissaire est tenu de rendre une décision dans les meilleurs délais (al. 20(3)a) de la LCR et nouvel art. 11.22 de la Loi sur le SCRS, ajouté à l'article 97 du projet de loi). À l'article 94 du projet de loi, une interrogation est définie comme étant une « recherche ciblée dans un ou plusieurs ensembles de données, au sujet d'une personne ou d'une entité, ayant pour but d'obtenir des renseignements ».

Selon l'article 22 de la LCR, chaque année civile, le commissaire au renseignement est tenu de présenter au premier ministre un rapport sur ses activités. Le rapport doit comporter des statistiques sur les décisions du commissaire relativement à l'approbation, à la modification ou au rejet des autorisations et des déterminations. Il revient au commissaire de déterminer les statistiques qu'il convient d'intégrer au rapport annuel.

Avant que le rapport du commissaire au renseignement ne soit présenté au premier ministre, le directeur du SCRS et le chef du CST en vérifieront le contenu afin d'en retirer tout renseignement protégé par le secret professionnel de l'avocat ou du notaire ou par le privilège relatif au litige et tout renseignement qui pourrait porter atteinte à la sécurité nationale, à la défense nationale ou aux relations internationales. Lorsqu'il a reçu le rapport, le premier ministre doit en déposer une copie devant les deux Chambres du Parlement dans les 15 premiers jours de séance de celles-ci.

2.3.1.3 Renseignements et ensembles de données accessibles au public

La collecte de renseignements accessibles au public par le CST et le SCRS n'est pas assujettie à une autorisation ou une détermination ministérielle ni à l'approbation du commissaire au renseignement. Aux fins de l'exercice de ses fonctions et attributions aux termes des articles 12 à 16 de la Loi sur le SCRS, le SCRS est autorisé, aux termes du nouveau paragraphe 11.11(1) de la Loi sur le SCRS, édicté à l'article 97 du projet de loi, à conserver, à interroger et à exploiter des ensembles de données accessibles au public sans détermination ministérielle ni approbation du commissaire au renseignement. De même, aux termes du paragraphe 23(1) de la Loi sur le CST, le CST est autorisé à acquérir, à utiliser, à analyser, à conserver et à divulguer de l'information accessible au public dans l'exécution de son mandat, et ce, sans détermination ministérielle ni approbation du commissaire au renseignement. L'utilisation du terme « divulguer » dans les nouveaux pouvoirs pour le CST donne à penser que des entités externes utiliseront les renseignements accessibles au public acquis et analysés par le CST, vraisemblablement dans le but d'en faire une pratique courante.

À l'article 2 sur la nouvelle Loi sur le CST du projet de loi C-59, l'expression « information accessible au public » est définie comme suit :

> Information publiée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information

> ou ailleurs ou disponible au public sur demande, par abonnement ou achat.

Il semblerait que cette définition permette l'acquisition massive de *toute* information accessible au public ayant été publiée ou diffusée aux fins de consommation publique, par exemple l'imagerie faciale saisie dans des publications sur les réseaux sociaux[28]. Il se pourrait donc que le CST et le SCRS puissent acquérir en masse de l'information accessible au public, ce qui signifie que les données ne seraient pas filtrées au préalable afin d'éliminer l'information non liée à la cible. En outre, les deux organismes seront habilités à analyser ou à exploiter l'information accessible au public qu'ils acquièrent, des activités qui donnent à penser que des connaissances seront découvertes par exploration de données. Comme la définition d'« information accessible au public » couvre aussi le paiement pour obtenir l'accès à des informations, des fournisseurs de services et des courtiers en information peuvent être encouragés à recueillir de nouvelles formes de dossiers d'information sur des utilisateurs pour les vendre au CST. Parmi les produits de courtiers en information déjà disponibles pour ceux qui sont disposés à payer, notons les antécédents de crédit, l'historique de navigation sur Internet, les achats en ligne, les contacts sur les réseaux sociaux, la situation matrimoniale et différents renseignements qui permettent la construction de profils personnels détaillés.

Si la collecte massive d'ensembles de données accessibles au public par le CST n'est pas soumise à la surveillance du commissaire au renseignement, d'autres activités du CST et du SCRS qui comportent la collecte et la conservation d'ensembles de données massifs relèveront de sa compétence. Ces activités comportent la collecte d'information non accessible au public (nouvel al. 26(2)b) de la Loi sur le CST et nouveaux art. 11.01 à 11.25 de la Loi sur le SCRS).

Dans le cas de la collecte de renseignements étrangers par le CST, des données sont parfois recueillies en masse, ce qui signifie que le CST acquiert de l'information pour des raisons techniques et opérationnelles sans utiliser de filtres précis liés à la cible de renseignements étrangers, comme des numéros de téléphone et des adresses électroniques. Étant donné l'imprévisibilité de l'acheminement des communications dans l'infrastructure mondiale de l'information[29] et l'absence de filtres dans le processus de collecte, des métadonnées canadiennes, comme des adresses de protocole Internet, peuvent être accessoirement recueillies dans ces ensembles de données étrangers. L'information ainsi acquise est qualifiée dans le projet de loi C-59 de « non sélectionnée », terme qui, en vertu de l'article 2 de la Loi sur le CST, désigne l'information « acquise, pour des raisons techniques ou opérationnelles, sans avoir recours à des termes ou des critères pour identifier l'information ayant un intérêt en matière de renseignement étranger[30] ». Selon le paragraphe 34(2) de la Loi sur le CST, pour approuver une autorisation ministérielle de recueillir des renseignements étrangers en masse, le commissaire au renseignement devra juger raisonnable la conclusion du ministre qu'aucun autre moyen raisonnable d'acquérir

l'information n'existe et que l'information relative à des Canadiens ou à des personnes se trouvant au Canada ne sera utilisée, analysée ou conservée que si elle est essentielle aux affaires internationales, à la défense ou à la sécurité.

Pour sa part, et sous réserve de l'approbation du commissaire au renseignement, le SCRS peut recueillir des catégories approuvées d'ensembles de données canadiens et est autorisé à conserver certains ensembles de données étrangers. Dans les amendements prévus au nouveau paragraphe 11.07(1) de la Loi sur le SCRS et édictés par l'article 97 du projet de loi, les renvois aux « catégories » d'ensembles de données dont l'évaluation et le classement pourraient prendre jusqu'à 90 jours peuvent indiquer que le SCRS exploitera l'analyse de « mégadonnées » pour s'acquitter de son mandat en matière de renseignement de sécurité.

2.4 PARTIE 3 : ÉDICTION DE LA LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (ART. 76)

2.4.1 Centre de la sécurité des télécommunications

L'article 76 du projet de loi retire de la *Loi sur la Défense nationale* (LDN) le mandat du CST et crée une loi habilitante distincte, la Loi constituant le Centre de la sécurité des télécommunications (titre agrégé : « Loi sur le Centre de la sécurité des télécommunications » [Loi sur le CST]). En gros, la Loi sur le CST confère au CST le pouvoir de recueillir en masse de l'information accessible au public, notamment de l'information sur les Canadiens, de recueillir des renseignements étrangers et de mener des opérations de réduction de la menace d'origine cybernétique contre des entités étrangères à l'aide de moyens secrets.

La nouvelle Loi sur le CST semble modifier l'objet des dispositions habilitantes pour le CST. La LDN établit des conditions strictes que doit respecter le CST pour déroger à la partie VI du *Code criminel*[31], qui interdit l'interception de communications privées, tandis que la Loi sur le CST établit les assises juridiques sur lesquelles le CST peut s'appuyer tant pour intercepter des communications privées que pour commettre une série beaucoup plus étendue d'infractions, dont la plupart ne sont pas précisées (art. 3 et 49 à 51 de la Loi sur le CST).

L'article 2 de la Loi sur le CST propose une définition des institutions fédérales visées par le mandat du CST, notamment le Parlement et ses institutions, les tribunaux fédéraux ainsi que les ministères et organismes fédéraux. Ainsi, le CST pourrait fournir des avis et des services en matière de cybersécurité à des organismes des trois organes du gouvernement. L'étendue de cette définition pourrait avoir des implications en ce qui concerne la séparation constitutionnelle des pouvoirs. Les tribunaux fédéraux et la Cour suprême du Canada ont menacé de lancer une contestation constitutionnelle au vu des efforts déployés par le gouvernement pour les

forcer à utiliser les services de technologie de l'information offerts par Services partagés Canada, ce qui comprend la surveillance de la cybersécurité par le CST, au motif que cela compromettrait leur indépendance [32].

Aux termes de l'article 4 de la Loi sur le CST, le gouverneur en conseil peut désigner, par décret, tout ministre fédéral comme responsable du CST. Il se pourrait donc que le ministre de la Défense nationale ne demeure pas le ministre responsable du CST.

2.4.1.1 Mandat

La Loi sur le CST élargit le mandat actuel du CST, qui passe de trois à cinq volets. Le CST est chargé actuellement d'acquérir des renseignements étrangers à partir de l'infrastructure mondiale de l'information, d'aider à protéger les renseignements et les réseaux électroniques du gouvernement et de fournir une assistance technique et opérationnelle aux agences fédérales d'application de la loi et de sécurité nationale, mais le paragraphe 15(2) de la Loi sur le CST vient ajouter au mandat du CST les cyberopérations défensives et actives.

L'article 47 de la Loi sur le CST, en ordonnant au ministre d'exercer personnellement les pouvoirs prévus aux paragraphes 26(1), 27(1), 27(2), 29(1), 30(1), 36(2), 39(1) et 40(1), veille à ce que le ministre ne puisse déléguer l'autorisation ou l'autorisation modifiée à l'égard de l'une ou l'autre des cinq activités confiées au CST.

Il convient de souligner que l'élargissement du mandat du CST touchant le renseignement étranger aux termes de l'article 16 englobe l'acquisition par des moyens secrets. Même si le CST déploie actuellement des efforts afin de dissimuler à ses cibles ses activités de collecte de données de renseignement étranger, l'autorisation explicite d'utiliser des moyens secrets ouvre la porte à une gamme beaucoup plus large de possibilités opérationnelles. Le nouvel alinéa 26(2)d) de la Loi sur le CST dit que le ministre peut autoriser le CST à « prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète » de l'activité de collecte de renseignements étrangers [33].

Les cyberopérations actives du CST pourraient aussi mettre à profit des moyens secrets. Bien que le mot « secret » ne soit pas employé à l'article 19 de la Loi sur le CST, où les cyberopérations actives sont décrites comme des activités dont le but est « de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités », le terme est employé à l'alinéa 31c), sous « Autorisations de cyberopérations ». Conformément à cette disposition, le CST peut « prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète » de ses cyberopérations actives.

Le fait d'autoriser le CST à mener des activités de réduction de la menace contre des cibles étrangères de façon indépendante du SCRS ne fait pas qu'élargir la portée d'intervention du gouvernement à l'égard de différents types de préoccupations – par exemple en matière de lutte contre les opérations et les mesures actives d'influence étrangère facilitées par les réseaux sociaux –, cela permet aussi au CST d'entreprendre de telles opérations en coopération avec des agences étrangères alliées.

Sous réserve de l'exception prévue au paragraphe 23(1) visant la collecte par le CST d'information accessible au public, l'article 22 de la Loi sur le CST dispose qu'aucune activité du CST ne peut viser des Canadiens ou des personnes se trouvant au Canada, contrevenir à la *Charte canadienne des droits et libertés* [34], ou être menée sans autorisation ministérielle. Il convient de souligner qu'une exception est aussi prévue à l'article 46 de la Loi sur le CST pour permettre au CST de mener des activités visant des Canadiens ou des personnes se trouvant au Canada afin de prévenir un danger imminent de mort ou de lésions corporelles graves.

2.4.1.2 Ententes

En ce qui concerne la coopération dans laquelle le CST peut s'engager, l'article 54 de la Loi sur le CST l'autorise explicitement à conclure des ententes avec des entités canadiennes ou étrangères qui ont des pouvoirs et des fonctions semblables aux siens.

Le terme « entité » est défini comme suit à l'article 2 de la Loi sur le CST : « Personne, groupe, fiducie, société de personnes ou fonds, ou organisation ou association non dotée de la personnalité morale. La présente définition vise également les États, leurs subdivisions politiques et leurs organismes. » Par conséquent, en plus des organismes de renseignement électromagnétique, de renseignement humain ou de cybersécurité étrangers, des organismes internationaux et des institutions de ces derniers, cette définition englobe les institutions et les organismes canadiens. L'Échange canadien de menaces cybernétiques, ou ECMC, est une entité canadienne avec laquelle le CST a déjà établi une relation [35]. Le nouveau Centre canadien pour la cybersécurité, créé en vertu de la *Loi nº 1 d'exécution du budget de 2018* et en activité depuis le 1er octobre 2018, passera vraisemblablement des ententes de collaboration avec des partenaires des secteurs public et privé.

Afin de favoriser la réalisation des activités confiées au CST, l'article 54 de la Loi sur le CST autorise le CST à conclure des ententes non seulement aux fins de communication de l'information à ces entités, mais aussi de « coopération avec elles ». Ce libellé pourrait ouvrir la porte à des cyberopérations actives et défensives de la part du CST, par des moyens secrets, en coopération avec des organismes de renseignement électromagnétique étrangers. Aucune de ces opérations ne serait assujettie à l'examen et à l'approbation du commissaire au renseignement. Toutefois, en vertu des articles 29 et 30 de la Loi sur le CST, avant de conclure une entente avec

une institution ou une organisation étrangère, le CST doit obtenir l'approbation du ministre, lequel doit consulter au préalable le ministre des Affaires étrangères.

2.4.1.3 Cyberopérations défensives et actives

L'article 18 de la Loi sur le CST décrit les cyberopérations défensives comme étant des activités menées « dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin d'aider à protéger » l'information électronique et les infrastructures de l'information. Toutefois, le libellé du paragraphe 29(1) de la Loi sur le CST, qui précise que le ministre peut autoriser une cyberopération défensive « malgré toute autre loi fédérale ou loi d'un État étranger », donne à penser que les cyberopérations défensives pourraient ne pas être tout à fait passives. De telles opérations pourraient enfreindre des lois canadiennes et, à moins d'être menées avec le consentement d'un État hôte, elles contreviendraient presque assurément à des lois étrangères.

Conformément aux paragraphes 29(2) et 30(2) de la Loi sur le CST, le ministre ne peut autoriser de cyberopérations défensives et actives, respectivement, qu'après consultation du ministre des Affaires étrangères ou avec son consentement. Cette exigence laisse supposer que des opérations de cette nature comportent un risque pour les affaires internationales du Canada.

L'Énoncé concernant la *Charte* du ministère de la Justice au sujet de l'article 34 (ancien art. 33) de la Loi sur le CST semble étayer le point de vue selon lequel les étrangers et leurs biens ne bénéficieront pas du même degré de retenue opérationnelle que les Canadiens et leurs biens [36].

Bien que l'approbation préalable du commissaire au renseignement ne soit pas obligatoire aux termes de la Loi sur le CST pour mener des cyberopérations défensives ou actives, l'OSASNR sera habilité, en vertu de l'alinéa 8(1)a) de la Loi sur l'OSASNR, à mener un examen *ex post* (après le fait) de la légalité, du caractère raisonnable et de la nécessité de telles opérations.

Les paragraphes 27(1) et 27(2) de la Loi sur le CST établissent respectivement que le CST est autorisé à mener des opérations de cybersécurité afin d'aider à protéger des institutions et des infrastructures fédérales et non fédérales désignées par le ministre aux termes du paragraphe 21(1) de la Loi sur le CST comme « étant importante pour le gouvernement fédéral ». Autrement dit, le CST peut jouer un rôle plus direct dans la protection des infrastructures de l'information essentielles contrôlées et exploitées par le secteur privé, un pouvoir qu'il possède déjà en vertu de l'alinéa 273.64(1)b) de la LDN, mais qui, à ce jour, n'a pas été exercé de façon systématique.

L'article 32 de la Loi sur la CST interdit au CST de se livrer à certaines activités dans le cadre de ses cyberopérations défensives et actives. Le CST ne peut causer des lésions corporelles [37] à une personne ni entraver, détourner ou contrecarrer le cours de

la justice ou de la démocratie. Ce libellé calque la formulation utilisée à l'article 12.2 de la Loi sur le SCRS pour établir les dispositions visant la réduction de la menace, à une importante exception près : contrairement au SCRS, il n'est pas explicitement interdit au CST de violer l'intégrité sexuelle d'une personne.

2.4.1.4 Autorisations ministérielles

L'article 33 de la Loi sur le CST décrit les procédures à suivre pour demander une autorisation ministérielle et les conditions qui doivent être remplies pour que le ministre donne son autorisation.

Le paragraphe 33(3) de la Loi sur le CST précise que, lorsque le CST présente une demande d'autorisation ministérielle de participer à des activités de cybersécurité concernant une infrastructure non fédérale, il doit y joindre une demande écrite d'aide en matière de cybersécurité du propriétaire de l'infrastructure. Les ministères, les institutions parlementaires et les tribunaux fédéraux n'ont pas à présenter de demande écrite d'aide en matière de cybersécurité au SCT avant que celui-ci fournisse cette aide. Toutefois, parmi les conditions que le CST doit remplir avant que le ministre puisse conclure à l'existence de motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle, et qu'il est justifié d'autoriser des opérations de cybersécurité pour des institutions fédérales, le CST doit démontrer, en vertu de l'alinéa 34(3)b) de la Loi sur le CST, qu'il ne pourrait raisonnablement obtenir le consentement de toutes les personnes dont les renseignements peuvent être acquis dans le cadre de ses activités.

L'article 35 de la Loi sur le CST décrit le contenu des autorisations ministérielles demandées afin de mener des activités de collecte de renseignements étrangers (par. 26(1)), d'offrir son concours en matière de cybersécurité à des institutions fédérales ou non fédérales (par. 27(1) et 27(2)) et de mener des cyberopérations défensives (par. 29(1)) ou actives (par. 30(1)). Entre autres choses, cette description du contenu précise le « qui, quoi et quand » de l'autorisation, par exemple les activités ou les catégories d'activités que le CST est autorisé à mener; les personnes ou les catégories de personnes qui sont autorisées à mener ces activités ou catégories d'activités; et les dates de délivrance et d'expiration des autorisations. Les autorisations ministérielles doivent aussi préciser les modalités, conditions ou restrictions qu'impose le ministre, notamment les mesures de protection de la vie privée et de garantie du caractère raisonnable et de la proportionnalité des activités. Par exemple, l'alinéa 35f) de la Loi sur le CST exige que le CST indique si une activité de collecte de renseignements étrangers comportera la collecte massive de renseignements « ainsi que les conditions ou restrictions que le ministre estime souhaitables pour limiter l'utilisation, l'analyse et la conservation » de cette information « non sélectionnée ».

Le paragraphe 36(2) de la Loi sur le CST accorde au ministre le pouvoir de prolonger jusqu'à un an la période de validité d'une autorisation de renseignement étranger ou

de cybersécurité. Bien qu'en vertu du paragraphe 36(3), la décision du ministre de prolonger la période de validité de l'autorisation délivrée ne soit pas assujettie à l'examen du commissaire au renseignement, le paragraphe 36(4) exige que le ministre avise dès que possible le commissaire au renseignement de toute prolongation de ce type.

Le paragraphe 37(1) de la Loi sur le CST dit que si des faits exposés dans la demande changent considérablement, le chef du CST doit en aviser le ministre dès que possible. Le paragraphe 37(2) de cette même loi accorde au ministre un pouvoir discrétionnaire quant au signalement des changements factuels au commissaire au renseignement, enjoignant au ministre de lui signaler de tels changements seulement si l'autorisation doit être soumise à l'approbation du commissaire au renseignement et s'il conclut que les changements sont importants.

Le paragraphe 37(3) de la Loi sur le CST dispose que si le ministre conclut que les faits sur lesquels une autorisation de cyberopérations actives ou défensives non assujettie à l'approbation du commissaire au renseignement ont considérablement changé, le ministre doit en aviser l'OSASNR.

Si le ministre conclut que les faits sur lesquels une autorisation était fondée ont considérablement changé, l'article 39 de la Loi sur le CST offre la possibilité de produire une autorisation modifiée et de la soumettre à l'examen et à l'approbation du commissaire au renseignement. Il convient de noter qu'aux termes du paragraphe 39(3) de cette même loi, une activité de renseignement étranger ou de cybersécurité menée en vertu d'une autorisation devant être modifiée parce que des faits ont considérablement changé demeure valide jusqu'à ce qu'une autorisation modifiée approuvée par le commissaire au renseignement entre en vigueur.

2.4.1.5 Autorisation de renseignement étranger ou de cybersécurité en cas d'urgence

L'article 40 de la Loi sur le CST habilite le ministre à délivrer une autorisation de renseignement étranger ou de cybersécurité en cas d'urgence s'il conclut qu'il y a des motifs raisonnables de croire que les conditions nécessaires pour autoriser de telles activités ont été remplies, mais que le temps requis pour obtenir l'approbation du commissaire au renseignement rendrait inutile la délivrance d'une autorisation selon les procédures habituelles. Le paragraphe 40(2) de la Loi sur le CST précise que le commissaire au renseignement n'est pas autorisé à examiner une autorisation en cas d'urgence. Toutefois, selon les dispositions de l'article 41 de cette même loi, le commissaire au renseignement et l'OSASNR doivent être avisés de toutes les autorisations en cas d'urgence dès que possible et, comme le précise l'article 42 de la Loi sur le CST, les autorisations en question ne sont valides que pour une période maximale de cinq jours.

En ce qui concerne la procédure, une demande d'autorisation en cas d'urgence adressée au ministre diffère de celle présentée dans des situations ordinaires à un égard : le paragraphe 40(3) de la Loi sur le CST précise qu'elle peut être faite oralement et qu'elle doit fournir au ministre des motifs raisonnables de croire que le temps requis pour obtenir l'approbation du commissaire au renseignement rendrait inutile la délivrance de l'autorisation selon les procédures habituelles.

Même si une demande d'autorisation de cybersécurité en cas d'urgence pour consulter et acquérir des renseignements d'une infrastructure non fédérale est faite oralement, le paragraphe 40(4) de la Loi sur le CST exige que le propriétaire ou l'exploitant d'une infrastructure de l'information non fédérale présente au ministre une demande écrite à cet égard.

2.4.1.6 Protection de la vie privée

L'article 24 de la Loi sur le CST exige que le CST prenne des mesures afin de protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à la conservation, à l'analyse et à la divulgation de l'information *acquise* dans le cadre de ses activités de collecte de renseignements étrangers, de cybersécurité ou de collecte d'information accessible au public. Ce libellé mérite d'être relevé, parce qu'il étend le régime de protection de la vie privée en vigueur du CST aux non-citoyens qui se trouvent au Canada.

Nous mettons ci-dessus l'accent sur le terme « acquise » pour attirer l'attention sur une distinction importante entre le mandat actuel et le nouveau mandat du CST. L'utilisation du terme « acquise » dans le nouveau mandat pourrait donner suite aux préoccupations que le commissaire du CST et le commissaire à la vie privée avaient soulevées au sujet du libellé ambigu de la LDN et de la façon dont le CST collecte et communique les métadonnées[38].

Le terme « acquérir » est employé dans le mandat actuel du CST pour les activités de collecte de renseignements étrangers. Plus particulièrement, l'alinéa 273.64(1)a) de la LDN confère le mandat suivant au CST : « *acquérir* et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers » [SOULIGNÉ PAR LES AUTEURS]. Toutefois, un autre terme est employé pour préciser le type d'information à l'égard duquel le CST doit prendre des mesures de protection de la vie privée. Le paragraphe 273.64(2) de la LDN oblige le CST à prendre des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements *interceptés* [SOULIGNÉ PAR LES AUTEURS]. Bien qu'aucune définition des termes « acquérir » et « intercepter » ne soit fournie dans le mandat actuel du CST, l'interception d'une communication privée est définie à l'article 183 du *Code criminel* comme incluant le « fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet ».

Le terme « prendre connaissance », dans la définition du *Code criminel*, renvoie à l'acte d'obtenir une communication, mais il désigne aussi le fait de reconnaître le sens ou l'importance de la communication, ce qui implique une étape qui survient après la collecte de l'information. À une époque, il allait sans dire que la reconnaissance du sens ou de l'importance d'une communication était une tâche effectuée par un humain, mais avec l'arrivée de l'intelligence artificielle, ce n'est plus forcément le cas. La presse britannique a cité des dirigeants du Government Communications Headquarters du Royaume-Uni (le pendant du CST) disant que l'interaction humaine est le point où les préoccupations relatives à la vie privée sont soulevées :

> L'interception d'une communication qui circule dans un câble de fibre optique n'implique pas une atteinte substantielle à la vie privée […] à moins que la communication soit sélectionnée aux fins d'examen : autrement dit, à moins qu'un humain ne l'examine ou puisse potentiellement l'examiner[39].

De même, le British Security Service (le pendant du SCRS au Royaume-Uni) utilise la même logique, en disant au Investigatory Powers Tribunal (tribunal des pouvoirs d'enquête) :

> Il convient aussi de souligner que, comme les ensembles de données personnelles en vrac font l'objet d'une recherche électronique, il y a inévitablement une intrusion nettement moins importante dans la vie privée des personnes concernées, puisque les données qui ne produisent pas de « concordance » ne seront pas consultées par l'opérateur humain du système, mais feront seulement l'objet d'une recherche électronique[40].

D'après le libellé de l'alinéa 273.64(1)a) et du paragraphe 273.64(2) de la LDN, le CST semble aussi faire une distinction entre l'acquisition d'information et son interception. Essentiellement, l'information que le CST acquiert en vertu de ses mandats touchant le renseignement étranger et la cybersécurité n'est considérée comme étant interceptée que lorsqu'un humain (souvent aidé d'une machine) a interagi avec elle d'une quelconque façon afin de reconnaître sa substance, son sens ou son importance. Cette interprétation concorderait avec l'argument de longue date du CST selon lequel, avant l'interception, il ne peut prédire si l'information qu'il aura acquise en vertu de son mandat touchant le renseignement étranger renferme des communications privées. Par conséquent, selon le mandat actuel du CST, l'information acquise par des moyens automatisés et conservée dans un tampon de données n'est pas considérée comme étant interceptée avant qu'un analyste ne l'interroge à l'aide d'un outil de recherche.

2.4.1.7 Communication d'informations

L'article 43 de la Loi sur le CST permet au CST de communiquer à des personnes ou à des catégories de personnes désignées par le ministre aux termes de l'article 45 de cette même loi toute information qui pourrait être utilisée pour identifier un Canadien ou une personne se trouvant au Canada – essentiellement, des métadonnées –, recueillie en vertu du volet du mandat touchant le renseignement étranger que lui confère le paragraphe 26(1) de la Loi sur le CST. Pour déterminer s'il devrait communiquer cette information, le CST doit conclure que la communication est essentielle « aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité ». Ce critère d'essentialité semble regrouper des éléments des critères d'essentialité prévus aux alinéas 273.65(2)d) et 273.65(4)d) de la LDN, que le CST applique actuellement aux communications qu'il fait dans le cadre des volets du mandat touchant le renseignement étranger et la cybersécurité.

Afin d'aider à protéger l'information électronique et les infrastructures de l'information fédérales et désignées, l'article 44 de la Loi sur le CST prévoit la communication de métadonnées et de communications privées interceptées (contenu). Cette disposition tient compte du fait que des codes malveillants utilisés dans des cyberattaques sont souvent incorporés dans le contenu de courriels ou de pièces jointes à un courriel, lesquels constituent des communications privées.

Le paragraphe 46(1) de la Loi sur le CST autorise le CST à utiliser ou à analyser de l'information se rapportant à un Canadien ou à une personne se trouvant au Canada s'il a des motifs raisonnables de croire qu'il y a un danger imminent de mort ou de lésions corporelles graves pour une personne physique, et que l'information à cet égard est pertinente. Le paragraphe 46(2) de la Loi sur le CST autorise le CST à communiquer l'information « aux personnes appropriées » si la communication peut aider à prévenir la mort ou des lésions corporelles graves.

L'Énoncé concernant la *Charte* du ministère de la Justice sur l'article 46 (ancien art. 47) de la Loi sur le CST offre des renseignements supplémentaires. On y souligne que l'information qui donne au CST des motifs raisonnables de croire qu'il y a un danger imminent de mort ou de lésions corporelles graves « peut avoir été découverte accessoirement par le CST dans le cadre d'activités autorisées ou peut [avoir] été fournie par un autre organisme ou une autre personne[41] ». Si le CST a recueilli accessoirement de l'information sur un Canadien, c'est probablement par suite de ses activités de collecte de renseignements étrangers. Sinon, l'Énoncé concernant la *Charte* dit que l'information qui donne au CST des motifs raisonnables de croire qu'il y a un danger imminent pourrait provenir d'un autre organisme ou d'une personne. Les deux dernières sources devraient susciter des questions sur la crédibilité de l'information de l'autre organisme ou de la personne. L'information a-t-elle été obtenue sous la torture, par exemple, ou pourrait-elle être corroborée à l'aide d'autres sources?

Il est important de ne pas oublier que la communication d'informations prévue à l'article 46 de la Loi sur le CST donnera probablement lieu à des activités policières ou militaires. L'emploi de l'expression « motifs raisonnables de croire » dans cette disposition est une norme reconnue en droit criminel et indique que le CST doit avoir un degré élevé de certitude concernant le danger et la pertinence de l'information relative au danger. Cependant, il est tout aussi important de souligner que le seuil à atteindre pour que le CST communique l'information – à savoir que la communication « peut » aider à prévenir la mort ou des lésions corporelles graves – est beaucoup plus bas.

L'Énoncé concernant la *Charte* dit aussi que « [l]'utilisation et la communication d'information potentiellement privée dans de telles circonstances *pourraient* faire intervenir l'article 8 de la *Charte* » [SOULIGNÉ PAR LES AUTEURS]. L'article 8 de la *Charte* dit que « [c]hacun a droit à la protection contre les fouilles, les perquisitions et les saisies abusives ». L'utilisation du terme « pourraient » par le ministère de la Justice à l'égard de l'article 8 de la *Charte* permet une évaluation au cas par cas de la nature de l'information à communiquer (par exemple, s'agit-il du contenu d'une communication ou de métadonnées?) et de déterminer si l'utilisation proposée de l'information et sa divulgation par le CST constituent une fouille et une perquisition. Il faut aussi déterminer si la *Charte* s'applique à des activités extraterritoriales, et dans l'affirmative, de quelle façon.

D'après le libellé employé dans l'article 46 de la Loi sur le CST et dans l'Énoncé concernant la *Charte*, il semblerait que cet article permettra au CST, dans des situations d'urgence, de contourner les processus habituels de communication de renseignements nominatifs et de divulguer immédiatement les communications privées ou les métadonnées relatives à des Canadiens à des personnes, y compris des personnes qui travaillent pour des États étrangers ou des entités et des sociétés étrangères. L'énoncé du ministère de la Justice selon lequel l'objectif de prévention d'un danger imminent de mort ou de lésions corporelles graves « peut servir à justifier l'utilisation d'information déjà en la possession du CST » semble laisser entendre que le CST peut aussi légitimement, dans les circonstances, interroger ses dépôts d'informations recueillies en masse pour trouver d'autres renseignements susceptibles de se rapporter au danger imminent.

Le paragraphe 46(3) de la Loi sur le CST ordonne au chef du CST d'aviser le ministre par écrit dès que possible si le CST a utilisé, analysé ou communiqué de l'information en vertu des dispositions de l'article 46. Le ministre doit alors à son tour en aviser l'OSASNR, bien qu'aucun délai ne soit rattaché à cette exigence.

L'article 55 de la Loi sur le CST interdit la divulgation forcée dans une instance devant un tribunal de l'identité d'une personne ou d'une entité qui assiste ou a assisté le Centre de manière confidentielle. Cette interdiction contre la divulgation forcée

couvre toute information qui permettrait de découvrir cette identité. Un juge désigné de la Cour fédérale pourrait autoriser la divulgation seulement si :

- la personne ou l'entité n'a pas assisté le CST;
- l'identité des personnes ou des entités ne pourrait être découverte à partir de l'information à divulguer;
- l'information est nécessaire pour établir l'innocence de l'accusé dans une poursuite pour infraction.

2.4.1.8 Réglementation

En plus des pouvoirs de réglementation généraux, l'alinéa 60c) de la Loi sur le CST confère à l'exécutif le pouvoir de modifier, par règlement, « la définition de tout terme défini à l'article 2 ou aux paragraphes 23(5) ou 44(3) afin de répondre, de façon directe ou indirecte, aux changements technologiques ». Cette disposition permet essentiellement au gouvernement de modifier la Loi sur le CST au moyen de mesures législatives subordonnées, lesquelles sont assujetties à un examen parlementaire beaucoup moins rigoureux, effectué seulement après l'entrée en vigueur du règlement [42].

2.4.1.9 Responsabilité civile et criminelle

Les articles 49 à 51 de la Loi sur le CST confèrent une immunité pour une vaste gamme d'activités du CST. L'article 49 confère une immunité en matière civile et pénale à quiconque agit en conformité avec une autorisation ministérielle ou aide, de bonne foi, une personne qu'il croit, en se fondant sur des motifs raisonnables, agir ainsi. Par conséquent, si un employé du CST ou une personne qui facilite des activités de cybersécurité autorisées du CST cause des dommages à l'infrastructure d'un fournisseur de télécommunications, ce dernier ne pourra demander des dommages-intérêts.

L'article 50 de la Loi sur le CST met le CST à l'abri de toute responsabilité aux termes de la partie VI du *Code criminel* relativement à l'interception de communications privées obtenues en vertu d'une autorisation ministérielle et à l'utilisation, à l'analyse, à la conservation et à la divulgation qu'il en fait. L'article 51 de cette même loi exonère l'État de toute responsabilité aux termes de l'article 18 de la *Loi sur la responsabilité civile de l'État et le contentieux administratif* [43], qui se rapporte à l'utilisation ou à la divulgation de communications privées interceptées. Les articles 50 et 51 de la Loi sur le CST diffèrent peu des dispositions actuelles des articles 273.69 et 273.7 de la LDN.

2.4.1.10 Exigences en matière de production de rapports

L'article 52 de la Loi sur le CST renferme des exigences de production de rapports selon lesquelles le chef du CST doit fournir un rapport sur le résultat des activités menées au titre d'autorisations ministérielles dans les 90 jours suivant le dernier jour de validité. À son tour, le ministre doit en fournir copie au commissaire au renseignement et à l'OSASNR.

En vertu de l'article 59 de la Loi sur le CST, dans les trois mois suivant la fin de l'exercice, le CST doit publier un rapport annuel de ses activités pour l'année écoulée.

2.5 PARTIE 4 : MODIFICATIONS DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ* (ART. 92 À 111)

2.5.1 Ensembles de données

2.5.1.1 Contexte

La partie 4 du projet de loi modifie la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS) essentiellement afin de créer des régimes d'autorisations judiciaires et d'autorisations approuvées par le commissaire au renseignement encadrant la collecte et la conservation d'ensembles de données par le SCRS. L'un s'applique aux ensembles de données canadiens et l'autre aux ensembles de données étrangers.

L'article 2 modifié de la Loi sur le SCRS définit le terme « ensemble de données » comme étant un « [e]semble d'informations sauvegardées sous la forme d'un fichier numérique qui portent sur un sujet commun ». Un « ensemble de données canadien » concerne principalement des personnes se trouvant au Canada ou des Canadiens. Un « ensemble de données étranger » concerne principalement des non-Canadiens à l'extérieur du Canada ou des sociétés qui ne sont pas constituées au Canada et qui se trouvent à l'extérieur du Canada.

Les modifications apportées à la Loi sur le SCRS peuvent être vues en partie comme une réponse à l'arrêt *X (Re)*, dans lequel le juge de la Cour fédérale Simon Noël a conclu que le SCRS avait manqué à son obligation de franchise en n'informant pas la Cour que, pendant la décennie précédente, il conservait des données non liées à la cible recueillies en vertu d'un mandat[44]. La décision était fondée sur le fait que le SCRS stockait ces « données connexes » – essentiellement des métadonnées de communications de tiers, mais non leur contenu – dans son Centre d'analyse des données opérationnelles (CADO). Le personnel du CADO utilisait des outils informatiques pour analyser ces métadonnées ainsi que des données stockées dans d'autres dépôts du SCRS, et fournissait les renseignements en découlant aux enquêteurs du SCRS pour les aider dans leur travail.

Le juge Noël a conclu que la Loi sur le SCRS n'autorise le SCRS à recueillir et à conserver que les renseignements « strictement nécessaires » à l'exécution de son mandat. De plus, il a statué que les mandats délivrés aux termes de l'article 21 de la Loi sur le SCRS n'autorisent le SCRS qu'à recueillir des renseignements sur les menaces à la sécurité du Canada, au sens de l'article 2, et dans le contexte des pouvoirs prévus aux articles 12 à 16. Selon lui, la conservation de données connexes par le SCRS ne s'inscrit pas dans son champ de compétence législatif et ne respecte pas le mandat premier et les fonctions principales du SCRS, qui sont limités[45].

2.5.1.2 Collecte, conservation et création d'ensembles de données

En vertu du nouvel article 11.05 de la Loi sur le SCRS, édicté par l'article 97 du projet de loi C-59, le SCRS est autorisé à recueillir des ensembles de données s'il a des motifs raisonnables de croire que ceux-ci sont accessibles au public, qu'ils font partie d'une catégorie approuvée ou qu'ils comportent principalement des informations liées à des personnes qui ne sont pas des Canadiens et qui se trouvent à l'extérieur du Canada.

L'article 102 du projet de loi C-59 modifie l'article 21 de la Loi sur le SCRS afin de permettre au SCRS de demander une autorisation judiciaire pour conserver des renseignements recueillis de manière incidente lors de l'exécution d'un mandat délivré en application de l'article 12, et de les utiliser pour créer des ensembles de données. L'article 12 de la Loi sur le SCRS permet au SCRS de recueillir, d'analyser et de conserver des renseignements sur des activités dont on croit qu'elles représentent une menace envers la sécurité du Canada.

Pour autoriser la conservation de renseignements recueillis de manière incidente lors de l'exécution du mandat, le juge saisi de la demande doit être convaincu que les renseignements aideront le SCRS dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12, 12.1 et 16 de la Loi sur le SCRS :

- Comme on le précise ci-dessus, l'article 12 prévoit que le SCRS peut recueillir, analyser et conserver des informations et des renseignements sur les menaces à la sécurité du Canada et qu'il doit faire rapport de ces menaces au gouvernement du Canada.
- L'article 12.1 habilite le SCRS à prendre des mesures afin de réduire les menaces à la sécurité.
- L'article 16 autorise le SCRS à aider le ministre de la Défense nationale et le ministre des Affaires étrangères à recueillir des renseignements étrangers au Canada.

2.5.1.3 Ensemble de données accessibles au public

La collecte d'ensembles de données accessibles au public par le SCRS, lesquels sont définis aux nouveaux articles 11.01 et 11.07 de la Loi sur le SCRS comme étant de l'information « accessible au public au moment de sa collecte », n'est assujettie ni à un contrôle judiciaire ni à la surveillance du commissaire au renseignement. Toutefois, des limites sont imposées à la collecte de tels ensembles de données par le SCRS. Le nouveau paragraphe 11.11(1) de la Loi sur le SCRS dit que le SCRS ne peut conserver, interroger et exploiter un ensemble de données accessibles au public qu'aux fins prévues aux articles 12 à 16, lesquels concernent le mandat du SCRS. Le nouveau paragraphe 11.11(2) de la Loi sur le SCRS impose les mêmes restrictions rattachées au mandat quant à la conservation par le SCRS des résultats de toute interrogation ou exploitation d'ensembles de données accessibles au public. Comme on le définit à l'article 2 modifié de la Loi sur le SCRS, l'exploitation s'entend d'une « analyse informatique d'un ou de plusieurs ensembles de données ayant pour but d'obtenir des renseignements qui ne seraient pas autrement apparents ». Autrement dit, l'exploitation consiste en l'exploration de données à l'aide d'algorithmes (essentiellement des ensembles de règles) pour découvrir des tendances et des liens.

Le nouvel alinéa 11.24(1)a) de la Loi sur le SCRS oblige le SCRS à tenir des dossiers pour ses ensembles de données accessibles au public. Ces dossiers doivent fournir la justification de la collecte des ensembles de données, les détails relatifs à chaque exploitation ainsi que les résultats de ces exploitations ou interrogations, et préciser la disposition législative en vertu de laquelle les résultats de chaque exploitation ou interrogation ont été conservés. En vertu de l'alinéa 11.24(1)b), le SCRS est tenu de vérifier, de façon périodique et aléatoire, que les résultats d'interrogation et d'exploitation conservés l'ont été aux fins des articles 12 à 16 de la Loi sur le SCRS. Le nouvel article 11.25 de la Loi sur le SCRS précise que les résultats de ces vérifications doivent être communiqués à l'OSASNR.

2.5.1.4 Évaluation, conservation et destruction d'ensemble de données

Les nouveaux paragraphes 11.24(2) et 11.24(3) de la Loi sur le SCRS obligent le SCRS à tenir et à vérifier des dossiers à l'égard des catégories approuvées s'appliquant aux ensembles de données canadiens et étrangers, en y restreignant l'accès aux employés désignés. Comme pour les ensembles de données accessibles au public, les résultats des activités menées de façon périodique et aléatoire pour vérifier que l'information est conservée correctement doivent être communiqués à l'OSASNR. En outre, le nouvel article 11.25 de la Loi sur le SCRS précise que l'OSASNR doit être informé de toute extraction d'information d'un ensemble de données étranger qui, par sa nature ou ses attributs, se rapporte à un Canadien ou à une personne se trouvant au Canada.

L'un des problèmes que le juge Noël a soulevés dans la décision *X (Re)* (voir la section 2.5.1.1 du présent résumé législatif) était que le SCRS stockait de l'information, sans être autorisé à le faire dans certains cas, pour des périodes indéfinies. Selon le juge, pour respecter le mandat que lui confère la loi, le SCRS doit évaluer dès que possible les données qu'il a recueillies en vertu d'un mandat, afin que l'information que la loi ne l'autorise pas à conserver puisse être détruite sans délai. Les modifications que le projet de loi C-59 propose dans le nouveau paragraphe 11.07(1) de la Loi sur le SCRS semblent tenir compte de cette préoccupation.

Un employé désigné du SCRS doit évaluer et confirmer, dès que possible, mais au plus tard dans les 90 jours suivant la date de la collecte de l'ensemble, s'il s'agit :

> a) d'un ensemble de données accessible au public au moment de sa collecte;
>
> b) d'un ensemble de données comportant principalement des informations liées à des Canadiens ou à d'autres individus se trouvant au Canada;
>
> c) d'un ensemble de données comportant principalement des informations liées à un individu qui n'est pas Canadien qui se trouve à l'extérieur du Canada ou à une personne morale qui n'a pas été constituée ou prorogée sous le régime d'une loi fédérale ou provinciale et qui se trouve à l'extérieur du Canada.

Le nouveau paragraphe 11.07(6) de la Loi sur le SCRS exige que, pendant la période d'évaluation de l'ensemble de données, l'employé désigné supprime les renseignements personnels qui, selon le SCRS, ne sont pas pertinents dans le cadre de l'exercice de ses fonctions et dont la suppression ne nuira pas à l'intégrité de l'ensemble de données.

Conformément au nouvel alinéa 11.1(1)a) de la Loi sur le SCRS, et peu importe que l'ensemble de données soit canadien ou étranger, l'employé désigné doit supprimer toute information qui porte sur la santé physique ou mentale d'un individu et pour lequel il existe une attente raisonnable en matière de protection de la vie privée [46]. Si l'évaluation détermine qu'il s'agit d'un ensemble de données canadien, le nouvel alinéa 11.1(1)b) exige que l'employé désigné supprime toute information protégée par le secret professionnel de l'avocat. S'il s'agit d'un ensemble de données étranger, le nouvel alinéa 11.1(1)c) de la Loi sur le SCRS exige que l'employé désigné extraie de l'ensemble les informations qui, par leur nature ou leurs attributs, se rapportent à un Canadien ou à une personne se trouvant au Canada.

Si l'évaluation détermine qu'un ensemble de données étranger concerne principalement des Canadiens ou des personnes se trouvant au Canada, aux termes du nouveau paragraphe 11.07(2) de la Loi sur le SCRS, l'employé désigné doit alors déterminer si cet ensemble fait partie d'une catégorie approuvée d'ensembles de données. Aux termes du nouvel article 11.01 de la Loi sur le SCRS, une catégorie approuvée d'ensembles de données est un ensemble de données canadien dont la collecte a été autorisée par le ministre de la Sécurité publique et de la Protection civile et approuvée par le commissaire au renseignement. Si l'évaluation révèle que l'ensemble de données n'appartient pas à une catégorie approuvée, le SCRS doit soit le détruire immédiatement, soit demander au ministre d'établir une nouvelle catégorie à laquelle l'ensemble pourra appartenir.

En vertu du nouveau paragraphe 11.03(2) de la Loi sur le SCRS, lorsque le ministre examine une demande de nouvelle catégorie d'ensembles de données canadiens approuvés, il doit déterminer que l'exploitation ou l'interrogation de l'ensemble de données en question permettra de générer « des résultats pertinents en ce qui a trait à l'exercice des fonctions qui lui sont conférées en vertu des articles 12, 12.1 et 16 », qui se rapportent au mandat du SCRS en matière de collecte et d'analyse de renseignements de sécurité, à son mandat en matière de réduction de la menace et à son mandat de collecte de renseignements étrangers au Canada. Si le ministre détermine que la collecte de l'ensemble de données devrait être autorisée, il doit en aviser le commissaire au renseignement afin que ce dernier puisse examiner le caractère raisonnable de la détermination du ministre. On ne sait pas très bien si le ministre est tenu d'informer le commissaire au renseignement des cas où il a été déterminé que la collecte ne devrait pas être autorisée, mais le libellé du paragraphe 11.08(4) de la Loi sur le SCRS donne à penser que cela ne sera pas nécessaire.

Le nouveau paragraphe 11.07(3) de la Loi sur le SCRS précise que, durant la période d'évaluation et jusqu'à ce que le commissaire au renseignement approuve la détermination du ministre, le SCRS n'est pas autorisé à interroger ni à exploiter l'ensemble de données. Une autorisation peut être considérée comme étant valide seulement après que le commissaire au renseignement a approuvé la détermination dans une décision transmise par écrit au ministre compétent. Si le commissaire au renseignement ne juge pas raisonnables les conclusions qui ont abouti à une autorisation ou à une modification, il doit refuser l'approbation et motiver sa décision par écrit au ministre.

Si le SCRS souhaite conserver un ensemble de données canadien, il doit demander une autorisation judiciaire en vertu du nouvel article 11.13 de la Loi sur le SCRS. Pour délivrer une autorisation, le juge doit être convaincu que la conservation de l'ensemble de données aidera le SCRS dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12, 12.1 et 16 de la Loi sur le SCRS, et que le SCRS

en a extrait les renseignements qui se rapportent à la santé physique ou mentale d'une personne et ceux qui sont protégés par le secret professionnel de l'avocat ou du notaire. Le nouveau paragraphe 11.14(2) de la Loi sur le SCRS précise que ces autorisations seront valides pour une période maximale de deux ans.

Entre autres choses, le nouveau paragraphe 11.13(2) de la Loi sur le SCRS exige que la demande indique au juge si le directeur du SCRS ou un employé désigné a soulevé des préoccupations exceptionnelles ou nouvelles en matière de protection de la vie privée. Aux termes du nouveau paragraphe 11.14(1) de cette même loi, lorsque le juge délivre une autorisation, il doit préciser toute condition relative à l'interrogation ou à l'exploitation de l'ensemble de données ou à sa destruction. Il doit aussi préciser les conditions qu'il estime indiquées dans l'intérêt public.

Si le juge refuse d'autoriser la conservation, sous réserve de l'échéancier prévu pour exercer ou épuiser tous les droits d'appel, le nouveau paragraphe 11.15(1) de la Loi sur le SCRS exige que le SCRS détruise sans délai l'ensemble de données canadien.

En vertu du nouvel article 11.17 de la Loi sur le SCRS, le ministre ou une personne désignée peut décider d'autoriser la conservation d'un ensemble de données étranger [47]. L'autorisation est donnée pour une période maximale de cinq ans, calculée à partir de la date de son approbation par le commissaire au renseignement. Comme le précise le paragraphe 11.19(3) de la Loi sur le SCRS, si le SCRS n'a pas présenté une nouvelle demande d'autorisation en vue de conserver un ensemble de données étranger avant l'expiration de l'autorisation précédente, il doit détruire l'ensemble de données dans les 30 jours suivant la date d'expiration.

Avant d'autoriser la conservation de l'ensemble de données, le ministre ou l'employé désigné doivent conclure que :

- l'ensemble de données concerne principalement des personnes ou des sociétés étrangères;
- l'ensemble de données est susceptible d'aider le SCRS dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12, 12.1, 15 et 16 de la Loi sur le SCRS;
- le SCRS a supprimé toute information de l'ensemble de données qui porte sur la santé physique ou mentale d'un individu à l'égard de laquelle il existe une attente raisonnable en matière de vie privée et toute information qui, par sa nature ou ses attributs, se rapporte à un Canadien ou à une personne se trouvant au Canada.

2.5.1.5 Situation d'urgence

Le nouveau paragraphe 11.22(1) de la Loi sur le SCRS permet au directeur du SCRS d'autoriser l'interrogation, par un employé désigné, d'un ensemble de données canadien qui n'est pas visé par une autorisation judiciaire valide donnée en vertu de

l'article 11.13 ou d'un ensemble de données étranger qui n'est pas visé par une autorisation donnée en vertu de l'article 11.17 (ce qui signifie que le commissaire au renseignement n'a pas approuvé l'autorisation) s'il conclut :

- que l'ensemble de données a été recueilli en vertu du nouveau paragraphe 11.05(1) de la Loi sur le SCRS, lequel précise que le SCRS peut recueillir un ensemble de données seulement s'il est convaincu que cet ensemble est pertinent aux fins de l'exécution de ses tâches aux termes des articles 12 à 16;
- qu'une situation d'urgence exige l'interrogation de l'ensemble de données.

L'autorisation du directeur en vertu du nouvel article 11.22 de la Loi sur le SCRS n'est valide que lorsque le commissaire au renseignement l'a approuvée par écrit. Comme le prévoit le nouveau paragraphe 11.22(2), l'autorisation doit fournir une description de la situation d'urgence, de l'ensemble de données à interroger et des motifs pour lesquels le directeur conclut que l'interrogation produira vraisemblablement des renseignements qui préserveraient la vie ou la sécurité d'un individu ou des renseignements d'une importance considérable pour la sécurité nationale qui seraient perdus si le SCRS s'en tenait aux processus d'autorisation habituels.

Le nouveau paragraphe 11.22(2.1) de la Loi sur le SCRS dit que le SCRS ne peut conserver les résultats d'une interrogation d'un ensemble de données effectuée en situation d'urgence que si :

- ces résultats sont recueillis, analysés et conservés en vertu de l'article 12;
- leur conservation est strictement nécessaire pour aider le SCRS dans l'exercice des fonctions qui lui sont conférées en vertu de l'article 12.1;
- leur conservation est nécessaire afin de prêter assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères conformément à l'article 16 de la Loi sur le SCRS. En vertu de cet article, le SCRS peut aider le ministre de la Défense nationale ou le ministre des Affaires étrangères en recueillant des renseignements étrangers au Canada.

2.5.1.6 Interrogation ou exploitation potentiellement illégales d'ensembles de données

En vertu du nouveau paragraphe 27.1(1) de la Loi sur le SCRS, établi à l'article 107 du projet de loi, si l'OSASNR est d'avis que le SCRS a interrogé ou exploité illégalement un ensemble de données aux termes des nouveaux articles 11.11 (ensemble de données accessible au public) et 11.2 (ensembles de données qui contiennent des renseignements personnels qui, dans l'immédiat, ne sont pas directement liés à des activités représentant une menace pour le Canada), l'OSASNR peut remettre au directeur du SCRS les extraits d'un rapport produit en vertu de l'article 35 de la Loi sur l'OSASNR ainsi que toute autre information qui, à son avis, serait utile à la Cour fédérale dans le cadre d'un examen effectué en vertu du

paragraphe 27.1(4) de la Loi sur le SCRS. Aux termes du paragraphe 27.1(2) de la Loi sur le SCRS, l'OSASNR doit s'assurer que les documents présentés au directeur ne comportent pas d'informations protégées par le secret professionnel de l'avocat ou par le privilège relatif au litige. Le nouveau paragraphe 27.1(3) de la Loi sur le SCRS indique que, dès que possible après la réception de ces informations, le directeur les fait déposer à la Cour fédérale avec toute autre information qu'il juge pertinente[48].

2.5.2 Mesures de réduction de la menace

L'article 98 du projet de loi modifie le paragraphe 12.1(2) de la Loi sur le SCRS de façon à exiger que les conséquences raisonnablement prévisibles sur les tierces parties, notamment sur leur droit à la vie privée, soient prises en compte lorsqu'on envisage de prendre des mesures pour réduire la menace.

Le paragraphe 12.1(3) de la Loi sur le SCRS est remplacé par un certain nombre de dispositions qui, entre autres choses, soulignent que la *Charte canadienne des droits et libertés* est la loi suprême du Canada et confirment que le SCRS ne peut prendre des mesures qui limiteraient un droit garanti par la *Charte* sans autorisation en vertu d'un mandat. En outre, un juge ne peut délivrer un tel mandat que s'il est convaincu que les mesures qu'il autorise sont conformes à la *Charte*.

Le nouveau paragraphe 12.1(3.4) de la Loi sur le SCRS insiste sur l'importance de la conformité à la loi en précisant que le SCRS ne peut prendre des mesures qui seraient par ailleurs contraires au droit canadien que si elles ont été autorisées par un mandat délivré au titre de l'article 21.1 de la Loi sur le SCRS.

Le nouveau paragraphe 12.1(3.5) de la Loi sur le SCRS crée, pour le SCRS, l'obligation d'aviser l'OSASNR qu'il a pris des mesures de réduction de la menace « [d]ans les plus brefs délais possible ».

L'article 99 du projet de loi resserre les restrictions que le paragraphe 12.2(1) de la Loi sur le SCRS impose à l'égard des mesures de réduction de la menace du SCRS de façon à inclure des interdictions contre la torture, la détention ou le fait de causer la perte de biens ou des dommages importants à ceux-ci si cela pouvait porter atteinte à la sécurité d'un individu.

L'article 103 du projet de loi modifie le paragraphe 21.1(1) de la Loi sur le SCRS, lequel traite des demandes de mandats concernant des mesures visant à réduire les menaces envers la sécurité du Canada. Entre autres choses, les modifications précisent que les mesures de réduction des menaces consistent notamment à : « modifier, enlever, remplacer, détruire, détériorer ou fournir tout ou partie d'un objet, notamment des registres, des documents, des biens, des composants et du matériel, ou en entraver la livraison ou l'utilisation » et à se faire passer pour une autre personne, à l'exception d'un policier, dans le but de prendre l'une de ces mesures.

Les alinéas 21.1(2)c) et 22.1(1)b) et l'article 22.2 modifiés de la Loi sur le SCRS (art. 103 à 105 du projet de loi) ajoutent chacun un libellé pour exiger que les conséquences sur les droits de tierces parties, notamment leur droit à la vie privée, soient prises en compte dans l'examen du caractère raisonnable et de la proportionnalité des mesures visant à réduire la menace.

2.5.3 Exonération de responsabilité pour des activités secrètes

Le nouveau paragraphe 18.2(1) de la Loi sur le SCRS, ajouté à l'article 100 du projet de loi, crée différentes exemptions à l'application du *Code criminel* afin d'exonérer de responsabilité les employés du SCRS et les personnes agissant sous la direction du SCRS si, dans le seul but de préserver une identité cachée :

- ils font une déclaration fausse au sujet d'une identité cachée;
- ils font un faux document ou ils font faire, demandent, possèdent, utilisent ou transmettent un tel document;
- ils déclarent qu'un faux document est authentique ou agissent comme s'il l'était.

Des dispositions supplémentaires semblent destinées à renforcer la responsabilisation à l'égard de l'utilisation des nouveaux pouvoirs de collecte d'informations et de renseignements du SCRS, en particulier la participation à des activités secrètes.

Entre autres choses, l'article 101 du projet de loi ajoute l'article 20.1 à la Loi sur le SCRS. Ces dispositions renforcent celles de l'article 20 de la Loi sur le SCRS relativement à la protection et à la conduite d'employés du SCRS, de façon à exiger, en vertu du paragraphe 20.1(3) de la Loi sur le SCRS, que le ministre détermine, par arrêté et au moins une fois par année :

> les catégories d'actes ou d'omissions qui constitueraient par ailleurs des infractions et qu'un employé désigné pourrait être justifié de commettre – ou dont il pourrait être justifié d'ordonner la commission –, s'il conclut que la commission de ces actes ou omissions est raisonnable.

Autrement dit, le ministre doit dresser une liste des types de lois que certains employés du SCRS ou personnes agissant sous leur direction seront autorisés à enfreindre dans l'exécution de leur mandat.

Aux termes des paragraphes 20(2) et 20(3) de la Loi sur le SCRS, le directeur est tenu de soumettre un rapport au ministre et d'en faire parvenir copie au procureur général s'il est d'avis qu'un employé a agi de façon illégale dans l'exercice des fonctions du SCRS. Toutefois, de tels actes et omissions seront parfois raisonnables, eu égard au rôle de l'employé dans l'exercice des fonctions du SCRS. Par exemple, il est illégal de dépasser les limites de vitesse, mais si un agent du renseignement du SCRS doit le faire pour maintenir la surveillance d'une personne que l'on croit sur le point d'achever la planification d'un attentat terroriste, cette illégalité peut être justifiée.

Selon les nouveaux paragraphes 20.1(3) et 20.1(5) de la Loi sur le SCRS, le caractère raisonnable de ces actes et omissions doit être évalué à la lumière des fonctions du SCRS en matière de collecte d'informations et de renseignements ainsi que de toute menace envers la sécurité du Canada à l'égard de laquelle des activités de collecte d'informations et de renseignements pourraient être menées ou de tout objectif de telles activités. Le commissaire au renseignement doit examiner et approuver les catégories d'actes ou d'omissions qui, selon la détermination du ministre, sont justifiées.

Comme le prévoient les paragraphes 20.1(6) et 20.1(7) de la Loi sur le SCRS, sur la recommandation du directeur, le ministre peut personnellement désigner des employés et des employés supérieurs qui, respectivement, recueillent des informations et des renseignements ou assument la responsabilité de ces activités, en application de l'article 20.1 de la Loi sur le SCRS. La période de validité de ces désignations ne peut dépasser un an.

En vertu du nouveau paragraphe 20.1(12) de la Loi sur le SCRS, le directeur ou un employé supérieur désigné est habilité à autoriser, par écrit et pendant un an maximum, des employés désignés à ordonner la perpétration d'actes et d'omissions qui constitueraient par ailleurs une infraction. Afin d'autoriser de telles actions, le directeur ou l'employé supérieur désigné doit avoir des motifs raisonnables de croire que les actes et les omissions sont raisonnables et proportionnels à la menace ou à l'objectif, eu égard à la disponibilité raisonnable d'autres moyens d'exécuter l'activité ou d'atteindre l'objectif.

Le nouveau paragraphe 20.1(23) de la Loi sur le SCRS prévoit que les employés désignés qui commettent des actes et des omissions ou qui en ordonnent la commission doivent soumettre un rapport écrit au directeur ou à un employé supérieur désigné dès que la situation le permet.

Le nouveau paragraphe 20.1(8) de la Loi sur le SCRS dispose aussi que, en situation d'urgence, le directeur ou un employé supérieur désigné peut désigner un employé pour une période maximale de 48 heures. Le ministre doit être avisé de la désignation dès que la situation le permet.

2.5.4 Rapport

Le nouveau paragraphe 20.2(1) de la Loi sur le SCRS, créé à l'article 101 du projet de loi, exige que le SCRS présente au ministre un rapport sur ses activités pour l'année précédente dans les trois mois suivant la fin de chaque année civile. Le ministre le fait ensuite déposer devant les deux Chambres du Parlement dans les 15 premiers jours de séance de celles-ci suivant sa réception.

Aux termes du nouveau paragraphe 20.1(24) de la Loi sur le SCRS, le ministre doit présenter chaque année un rapport public indiquant :

- le nombre de désignations effectuées en situation d'urgence;
- le nombre d'autorisations accordées à des employés désignés pour ordonner la commission d'actes et d'omissions;
- le nombre de fois où des employés désignés ont ordonné la commission d'actes et d'omissions en vertu de ces autorisations;
- la nature des menaces envers la sécurité à l'égard desquelles ont été menées les activités de collecte d'informations et de renseignements exigeant la commission d'actes et d'omissions;
- la nature des actes et des omissions qui ont été commis ou dont la commission a été ordonnée.

Comme le prévoit le nouveau paragraphe 20.1(25) de la Loi sur le SCRS, le rapport ne doit pas contenir de renseignements dont la communication, selon le cas :

- compromettrait une activité de collecte d'informations et de renseignements en cours ou nuirait à une telle activité;
- compromettrait l'identité d'un employé qui agit sous le couvert d'une identité cachée, l'identité d'une source humaine ou celle d'une personne agissant sous le couvert d'une telle identité et sous la direction d'un employé;
- mettrait en danger la vie ou la sécurité d'un individu;
- porterait atteinte à une procédure judiciaire;
- serait contraire à l'intérêt public.

Selon le nouveau paragraphe 20.1(26) de la Loi sur le SCRS, le SCRS doit, « [d]ans les plus brefs délais possible » après l'établissement d'une désignation en situation d'urgence, informer l'OSASNR qu'un employé désigné est autorisé à commettre des actes ou des omissions, ou qu'un rapport écrit est présenté au directeur du SCRS ou à un employé supérieur désigné pour l'informer des actes ou omissions commis ou ordonnés par un employé désigné.

2.6 PARTIE 5 : MODIFICATIONS DE LA *LOI SUR LA COMMUNICATION D'INFORMATION AYANT TRAIT À LA SÉCURITÉ DU CANADA* (ART. 112 À 126)

2.6.1 Contexte

2.6.1.1 Description générale de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*

La *Loi sur la communication d'information ayant trait à la sécurité du Canada*[49] (LCISC) était l'une des lois édictées par le projet de loi C-51, c'est-à-dire la *Loi antiterroriste de 2015*[50], qui a reçu la sanction royale en juin 2015.

La LCISC a essentiellement établi des pouvoirs explicites de communication d'information entre les institutions fédérales pour des considérations de sécurité nationale. Plus précisément, elle a pour « objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication, afin de protéger le Canada contre des activités portant atteinte à la sécurité du Canada[51] ».

Le paragraphe 5(1) de la LCISC a instauré un nouveau pouvoir discrétionnaire pour les institutions fédérales en matière de communication d'information à l'égard d'activités portant atteinte à la sécurité du Canada :

> 5(1) Sous réserve des dispositions de toute autre loi fédérale ou de tout règlement pris en vertu de l'une de celles-ci interdisant ou restreignant la communication d'information, une *institution fédérale* peut, de sa propre initiative ou sur demande, *communiquer de l'information* au responsable d'une *institution fédérale destinataire* dont le titre figure à l'annexe 3, ou à son délégué, si l'information se rapporte à la compétence ou aux attributions de l'institution destinataire prévues par une loi fédérale ou une autre autorité légitime à l'égard *d'activités portant atteinte à la sécurité du Canada*, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention ou la perturbation de ces activités ou une enquête sur celles-ci [SOULIGNÉ PAR LES AUTEURS].

La notion d'institution fédérale est définie à l'article 2 de la LCISC et englobe :

- tout ministère ou département d'État relevant du gouvernement du Canada, ou tout organisme, figurant à l'annexe de la *Loi sur la protection des renseignements personnels*;
- toute société d'État mère ou filiale à cent pour cent d'une telle société, au sens de l'article 83 de la *Loi sur la gestion des finances publiques*.

Les 17 institutions fédérales destinataires sont énumérées à l'annexe 3 de la LCISC[52].

2.6.1.2 Réforme de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*

2.6.1.2.1 Études réalisées par des comités de la Chambre des communes

Deux comités de la Chambre des communes ont réalisé des études touchant la LCISC en concomitance avec les consultations sur la sécurité nationale lancées par le gouvernement en septembre 2016.

En juin 2016, le Comité permanent de la sécurité publique et nationale de la Chambre des communes (SECU) a réalisé une étude portant sur le cadre de la sécurité nationale du Canada[53]. En mai 2017, le Comité SECU a publié son rapport, intitulé *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale du Canada*, lequel était accompagné de recommandations, dont cinq concernant une réforme de la LCISC[54].

En octobre 2016, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (ETHI) a décidé d'entreprendre une étude de la LCISC, des répercussions qu'elle a eues sur la vie privée depuis sa mise en œuvre et des modifications qui pourraient être proposées au cours des consultations du gouvernement sur la sécurité nationale[55]. En mai 2017, le Comité ETHI a publié son rapport intitulé *Assurer la sécurité nationale du Canada tout en protégeant le droit à la vie privée des Canadiens : Examen de la Loi sur la communication d'information ayant trait à la sécurité du Canada (LCISC)* [56]. Le rapport comportait un certain nombre de recommandations visant à modifier la LCISC.

2.6.1.2.2 Consultations du gouvernement du Canada

Dans le cadre de ses consultations sur la sécurité nationale, le gouvernement du Canada a publié le rapport intitulé *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016*, qui visait à « engager une discussion et un débat au sujet du cadre de sécurité nationale du Canada, afin d'informer des changements de politique qui seront apportés à la suite du processus de consultation[57] ». Ce rapport comportait une section sur la communication d'information sur la sécurité nationale entre les institutions gouvernementales, dont la communication d'information assujettie à la LCISC.

Le rapport sur les résultats des consultations précise que les pouvoirs accrus concernant la communication d'information entre les institutions fédérales en vertu de la LCISC ont soulevé de nombreuses préoccupations. Plus particulièrement :

> [d]e nombreuses organisations ont recommandé que la LCISC soit abrogée ou révisée en profondeur, se disant préoccupées – en particulier parmi les organisations de défense des droits de la personne ainsi que les organisations juridiques et communautaires – par le fait que les définitions actuelles de l'information pouvant ou ne pouvant pas être communiquée sont trop vagues et que les

> mécanismes d'examen existants n'offrent pas une responsabilisation adéquate[58].

En ce qui a trait à la LCISC, la plupart des participants aux consultations ont appuyé :

- un renforcement de la surveillance de la LCISC afin de protéger la vie privée;
- un renforcement de la surveillance de la LCISC afin de s'assurer que les institutions fédérales destinataires utilisent l'information communiquée de manière licite et conformément aux règles qui leur sont applicables seulement;
- « la tenue de dossiers détaillés sur les communications effectuées lors de la communication d'information » en vertu de la LCISC;
- la réduction du nombre d'institutions fédérales destinataires « à celles qui ont un mandat fondamental en matière de sécurité nationale »;
- l'inclusion à la LCISC d'une définition plus précise des « activités de défense d'une cause, de protestation, de manifestation d'un désaccord ou d'expression artistique »;
- la clarification de ce que constitue une « activité portant atteinte à la sécurité du Canada »;
- l'inclusion à la LCISC d'une clarification précisant que « les institutions qui reçoivent de l'information sur la sécurité nationale ne doivent l'utiliser que dans les limites permises par les lois qui s'appliquent à elles, dont la *Loi sur la protection des renseignements personnels* »;
- l'élaboration de « nouveaux règlements pour obliger les institutions à tenir un dossier sur les communications effectuées en vertu de la LCISC afin d'assurer une responsabilisation adéquate[59] ».

2.6.2 Modifications de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* prévues dans le projet de loi C-59

2.6.2.1 Remplacement du terme « sharing » par « disclosure » dans la version anglaise de la LCISC (art. 112, 113, 114 et 116 et par. 117(1) et 117(3))

La version anglaise du sommaire du projet de loi C-59 précise que la LCISC est modifiée dans le but suivant : « emphasize that the Act addresses only the disclosure of information and not its collection or use ». En conséquence, le terme « information sharing » est remplacé par « disclosure of information » ou « information disclosure » à divers endroits dans la version anglaise de la LCISC, notamment dans les dispositions suivantes : articles 112 et 114, dans le titre intégral et le titre abrégé de la LCISC; article 116, dans le texte décrivant l'objet de la LCISC; article 113 et paragraphes 117(1) et 117(3). L'expression française *communication d'information* (et ses variantes) demeure.

2.6.2.2 Préambule (par. 113(2))

Le paragraphe 113(2) du projet de loi modifie le préambule de la LCISC de manière à préciser que la communication d'information doit se faire en conformité avec la *Loi sur la protection des renseignements personnels* et d'autres lois, ainsi qu'avec la *Charte canadienne des droits et libertés*.

Le huitième paragraphe du préambule est modifié de manière à préciser qu'un pouvoir explicite « facilitera la communication d'information responsable et efficace, de façon à protéger la sécurité du Canada ».

2.6.2.3 Définitions (art. 115)

L'article 115 du projet de loi modifie l'article 2 de la LCISC, lequel établit les définitions qui se rattachent à la LCISC.

Le paragraphe 115(1) du projet de loi abroge la définition du terme « population du Canada », actuellement défini comme suit :

> a) La population au Canada;
>
> b) tout citoyen, au sens du paragraphe 2(1) de la *Loi sur la citoyenneté*, ou tout résident permanent, au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés*, qui se trouve à l'étranger.

Parallèlement, le paragraphe 115(2) du projet de loi modifie la définition d'activité portant atteinte à la sécurité du Canada en supprimant le terme « population du Canada » et en précisant qu'une telle activité comprend les activités menaçant la vie ou la sécurité de la population au Canada ou de toute personne physique qui a un lien avec le Canada et qui se trouve à l'étranger. Ainsi, on vise les personnes qui se trouvent au Canada, peu importe leur nationalité, et les personnes qui ont un lien avec le Canada et qui se trouvent à l'étranger. La notion de « personne ayant un lien avec le Canada » n'est pas définie dans le projet de loi.

Le projet de loi modifie également l'alinéa a) de la définition « d'activité portant atteinte à la sécurité du Canada » de manière à en retirer les activités qui ont pour effet d'entraver la capacité du gouvernement fédéral en matière d'administration de la justice, de relations diplomatiques ou consulaires ou de stabilité économique ou financière du Canada.

Le paragraphe 115(4) du projet de loi modifie la LCISC afin de préciser qu'une activité portant atteinte à la sécurité du Canada inclut les activités de défense d'une cause, de protestation, de manifestation d'un désaccord ou d'expression artistique

seulement si elles ont un lien avec une activité portant atteinte à la sécurité du Canada [60].

2.6.2.4 Principes directeurs (par. 117(2))

Le paragraphe 117(2) du projet de loi modifie les principes directeurs énoncés à l'article 4 de la LCISC. Plus précisément, il modifie l'alinéa 4c) de la LCISC afin de préciser que la conclusion d'une entente de communication d'information convient lorsqu'une institution fédérale communique régulièrement de l'information à la même institution fédérale.

2.6.2.5 Modification du pouvoir de communication d'information (art. 118)

L'article 118 du projet de loi modifie le seuil relatif à la communication d'information d'une institution fédérale à une institution fédérale destinataire.

L'alinéa 5(1)a) modifié de la LCISC prévoit que la communication d'information doit aider :

> à l'exercice de la compétence ou des attributions de l'institution fédérale destinataire prévues par une loi fédérale ou une autre autorité légitime à l'égard d'activités portant atteinte à la sécurité du Canada.

En outre, l'alinéa 5(1)b) de la LCISC, ajouté à l'article 118 du projet de loi, exige que l'incidence de la communication sur le droit à la vie privée d'une personne soit « limitée à ce qui est raisonnablement nécessaire dans les circonstances ».

Au cours de diverses consultations, des inquiétudes ont été soulevées quant au seuil de communication prévu par la LCISC – à savoir la pertinence –, et des recommandations ont été formulées à cet égard. Le commissaire à la protection de la vie privée, le Comité SECU et le Comité ETHI ont recommandé que le seuil de communication prévu à la LCISC soit élevé au seuil de la nécessité [61].

2.6.2.6 Fiabilité de l'information communiquée

L'article 118 du projet de loi modifie aussi le paragraphe 5(2) de la LCISC afin d'y inclure, à l'intention des institutions fédérales communiquant de l'information, une obligation légale de fournir à l'institution destinataire des « renseignements sur l'exactitude de l'information et la fiabilité quant à la façon dont celle-ci a été obtenue ». Cette modification donne suite à la recommandation du Comité ETHI qui demandait « [q]ue le gouvernement du Canada modifie la *Loi sur la communication d'information ayant trait à la sécurité du Canada* afin de créer l'obligation légale d'assurer la fiabilité de l'information communiquée en vertu de la LCISC [62] ».

2.6.2.7 Obligation de détruire ou de remettre les renseignements personnels

Le nouvel article 5.1 de la LCISC oblige les institutions gouvernementales, dans certaines circonstances, à détruire ou à remettre les renseignements personnels reçus en vertu de la LCISC.

2.6.2.8 Conservation de documents (art. 119 et 120)

Le paragraphe 119(1) ajoute le paragraphe 9(1) à la LCISC afin d'établir, pour les institutions fédérales qui communiquent de l'information, l'obligation légale de conserver certains documents qui contiennent des renseignements administratifs sur l'information communiquée. Cette modification semble répondre aux préoccupations soulevées quant au fait que, si les documents ne sont pas conservés, le contrôle de l'information communiquée en vertu de la LCISC est impossible [63]. Le nouveau paragraphe 9(2) prévoit des dispositions semblables visant les institutions destinataires.

Le paragraphe 119(2) du projet de loi, qui ajoute le paragraphe 9(3) à la LCISC, prévoit un mécanisme de surveillance de la communication et de la réception d'information en vertu de la LCISC. Dans les 30 jours suivant la fin de l'année civile, chaque institution fédérale ayant communiqué ou reçu de l'information au cours de l'année doit présenter à l'OSASNR une copie des dossiers produits en application des paragraphes 9(1) et 9(2). À moins qu'un règlement soit pris aux termes de l'alinéa 9(1)f) de la LCISC ou de l'article 120 du projet de loi, la surveillance ne visera apparemment pas l'information du destinataire.

Le projet de loi modifie également l'article 10 de la LCISC afin d'autoriser la prise de règlement pour la conservation des documents dont il est question au paragraphe 119(1) du projet de loi.

2.7 PARTIE 6 : MODIFICATIONS DE LA *LOI SUR LA SÛRETÉ DES DÉPLACEMENTS AÉRIENS* (ART. 127 À 139)

2.7.1 Contexte

À la suite de l'édiction, en 2004, de la *Loi de 2002 sur la sécurité publique* [64], Transports Canada a créé, en juin 2007, le Programme de protection des passagers et la « Liste des personnes précisées » (LPP) s'y rapportant. Cette loi a donné lieu à plusieurs modifications de la *Loi sur l'aéronautique* [65], notamment l'adoption du paragraphe 4.81(1), qui autorise le ministre des Transports à demander à tout transporteur aérien de fournir des renseignements à l'égard de « toute personne qu'il précise ». Une fois communiqués, ces renseignements sont ajoutés à la LPP.

La *Loi antiterroriste de 2015* a élargi le Programme de protection des passagers en édictant la *Loi sur la sûreté des déplacements aériens* (LSDA)[66], laquelle a remplacé le cadre qui régissait l'inscription à la Liste des personnes précisées. La LSDA, au paragraphe 8(1), établit un cadre législatif autorisant le ministre de la Sécurité publique et de la Protection civile à dresser une liste de personnes (la LPP, communément appelée « liste d'interdiction de vol ») sur laquelle il peut inscrire le nom de toute personne dont on a des motifs raisonnables de soupçonner qu'elle :

- soit participera ou tentera de participer à un acte qui menacerait la sûreté des transports;
- soit se déplacera en aéronef dans le but de commettre une infraction de terrorisme précisée (participation aux activités d'un groupe terroriste, facilitation d'une activité terroriste ou perpétration d'une infraction pour le compte d'un groupe terroriste) ou de commettre un acte criminel dont l'acte ou l'omission constituent également une activité terroriste[67], au Canada ou à l'étranger.

Des Canadiens ont soulevé des préoccupations concernant l'efficacité du Programme de protection des passagers, l'inscription de personnes sur la liste, le nombre d'erreurs d'identification, l'absence d'un mécanisme de recours et la nécessité de renforcer les dispositions de recours administratifs et d'appels dans la LSDA. Ces questions étaient au nombre de celles soulevées au cours des consultations publiques sur la sécurité nationale lancées par le gouvernement du Canada en 2016 et de l'étude parallèle menée par le Comité SECU[68].

2.7.2 Liste des personnes précisées (art. 129)

L'article 129 du projet de loi modifie l'actuel article 8 de la LSDA afin de veiller à ce que tous les prénoms d'une personne soient inscrits sur la LPP ainsi que tout autre renseignement prévu par règlement permettant d'identifier cette personne.

2.7.3 Obligation des transporteurs aériens et communication de renseignements sur les passagers (art. 127)

La LSDA oblige à l'heure actuelle les transporteurs aériens ou les exploitants d'un système de réservation de services aériens à fournir tous les renseignements sur les passagers prévus à l'annexe de la *Loi sur l'aéronautique*[69] concernant les personnes qui sont ou seront vraisemblablement à bord d'un aéronef pour tout vol. Par la suite, l'Agence des services frontaliers du Canada (ASFC) recueille les renseignements sur les passagers et les compare à ceux figurant dans la LPP afin d'identifier une personne inscrite sur la liste qui tente de prendre l'avion. En vertu de l'actuel article 14 de la LSDA, l'ASFC peut ensuite informer les transporteurs aériens et les exploitants de systèmes de réservation de services aériens que le nom d'un passager est le même que celui d'une personne inscrite sur la liste.

L'article 127 du projet de loi C-59 modifie le paragraphe 6(2) de la LSDA afin de le rendre conforme aux modifications apportées à l'article 8 de cette même loi. Par conséquent, un transporteur aérien doit aussi fournir tous les prénoms des personnes et tout autre renseignement prévu par règlement qu'il a en sa possession. Les autres éléments énumérés sont le prénom et le nom des personnes, leur date de naissance et leur sexe. Le délai et le mode de transmission de l'information seront fixés par règlement.

De plus, le nouveau paragraphe 6(4) de la LSDA modifie le cadre juridique qui oblige les transporteurs aériens et les exploitants d'un système de réservation de services aériens à fournir les renseignements en leur possession soit au ministre de la Sécurité publique et de la Protection civile soit au ministre des Transports sur demande. La portée de l'obligation de fournir des renseignements sur demande est limitée aux renseignements sur les passagers inscrits prévus à l'annexe de la *Loi sur l'aéronautique*, mais elle peut être élargie de façon à inclure d'autres renseignements prescrits par règlement. Aux termes du nouveau paragraphe 6(5), les renseignements demandés ne peuvent concerner qu'une personne inscrite ou une personne à l'égard de laquelle il y a des raisons de croire qu'il s'agit d'une personne inscrite.

L'actuel article 10 de la LSDA prévoit le cadre dans lequel les autorités ci-dessous peuvent prêter assistance au ministre de la Sécurité publique et de la Protection civile :

> a) le ministre des Transports;
>
> b) le ministre de la Citoyenneté et de l'Immigration;
>
> c) un membre de la Gendarmerie royale du Canada ou un membre du personnel civil de celle-ci;
>
> d) le directeur ou un employé du Service canadien du renseignement de sécurité;
>
> e) un dirigeant ou un employé de l'Agence des services frontaliers du Canada;
>
> f) toute autre personne ou entité réglementaire.

Le nouveau paragraphe 6(6) de la LSDA limite la portée des renseignements que peuvent demander les personnes désignées aux alinéas 10b) à 10f) de la LSDA, en leur donnant le pouvoir de demander aux transporteurs aériens seulement les renseignements énumérés à l'annexe de la *Loi sur l'aéronautique*[70] ou ceux qui sont prévus par règlement. Ici encore, les renseignements demandés ne peuvent concerner qu'une personne inscrite ou une personne à l'égard de laquelle il y a des raisons de croire qu'il s'agit d'une personne inscrite, et à la seule fin d'aider le ministre de la Sécurité publique et de la Protection civile dans l'application et l'exécution de la LSDA.

2.7.4 Collecte et communication d'information (art. 130)

2.7.4.1 Identifiant unique (vérification de l'identité avant le départ)

L'article 130 du projet de loi, dans le nouvel article 10.1 de la LSDA, introduit la notion d'un « identifiant unique » dans le cadre juridique de la LSDA. Le ministre de la Sécurité publique et de la Protection civile peut recueillir les renseignements personnels qu'un voyageur fournit afin de lui attribuer un identifiant unique pour faciliter la vérification de son identité avant un vol.

2.7.4.2 Collecte de renseignements sur les passagers aux fins d'identification

L'article 130 du projet de loi, dans le nouvel article 10.2 de la LSDA, confère au ministre de la Sécurité publique et de la Protection civile le pouvoir de recueillir des renseignements sur les passagers qui ont été ou sont réputés avoir été fournis en vertu des nouveaux paragraphes 6(2), 6(3) et 6(4) de la LSDA aux fins de l'identification des personnes inscrites qui sont ou seront vraisemblablement à bord d'un aéronef.

Comme indiqué précédemment, aux termes de l'article 10 de la LSDA, la LSDA fournit toujours un cadre pour la communication des renseignements recueillis sur les passagers entre des ministères et organismes fédéraux, notamment Transports Canada, Sécurité publique Canada, Immigration, Réfugiés et Citoyenneté Canada, la GRC, le SCRS et l'ASFC.

2.7.4.3 Communication de l'information

Comme indiqué ci-dessus, le cadre législatif pour la communication de l'information est élargi par les nouveaux paragraphes 6(2) et 6(3) de la LSDA. Le nouveau paragraphe 10.3 de la LSDA, qui permet la communication autorisée des renseignements sur les passagers obtenus ou réputés avoir été obtenus auprès de transporteurs aériens, habilite le ministre de la Sécurité publique et de la Protection civile à :

- communiquer des renseignements afin d'obtenir de l'assistance pour identifier les personnes inscrites qui sont ou seront vraisemblablement à bord d'un aéronef, si les renseignements concernent une personne à l'égard de laquelle le ministre a des raisons de croire qu'il s'agit d'une personne inscrite;
- communiquer des renseignements afin de se conformer soit à un subpoena, à un document ou à une ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements, soit à des règles de procédure se rapportant à la production de renseignements.

Le nouveau paragraphe 10.3(2) de la LSDA dit que le ministre de la Sécurité publique et de la Protection civile a toujours le pouvoir de communiquer de l'information pour assurer la sûreté des transports ou empêcher un déplacement aérien dont le but est de participer à une activité terroriste, selon ce que prévoit l'alinéa 8(1)b) de la LSDA. Si les renseignements concernent une personne inscrite, ils doivent avoir été obtenus ou réputés avoir été obtenus auprès du transporteur aérien en vertu des paragraphes 6(2) et 6(3) de la LSDA.

En outre, aux termes du nouvel article 11 de la LSDA, le ministre conserve le pouvoir de communiquer des renseignements obtenus dans l'exercice des attributions qui lui sont conférées au titre de la LSDA si la communication a pour but d'assurer la sûreté des transports ou de prévenir un déplacement aérien dont le but est de participer à une activité terroriste, pourvu qu'il ne s'agisse pas de renseignements fournis en vertu des paragraphes 6(2) ou 6(3) de la LSDA.

Le nouvel article 12 de la LSDA prévoit que le ministre peut, sous réserve d'un accord écrit, communiquer « tout renseignement qu'il est autorisé à communiquer au titre du paragraphe 10.3(2) ou de l'article 11 », ainsi que tout ou partie de la LPP au gouvernement d'un État étranger, à l'une de ses institutions ou à un organisme international. Ce dernier pouvoir de communication était déjà conféré au ministre en vertu de l'actuel article 12 de la LSDA.

Le nouvel article 12.1 de la LSDA dispose que le ministre peut communiquer au parent ou tuteur d'un enfant le fait que ce dernier n'est pas une personne inscrite.

2.7.5 Pouvoirs de communication de l'Agence des services frontaliers du Canada (art. 133)

L'article 133 du projet de loi C-59 élimine le pouvoir précédemment précisé de l'ASFC de communiquer à des transporteurs aériens et à des exploitants de systèmes de réservation de services aériens le fait que le nom d'un passager est le même que celui d'une personne inscrite. Selon l'article 14 modifié de la LSDA, l'ASFC n'est autorisée qu'à communiquer au ministre de la Sécurité publique et de la Protection civile (ou à toute autre personne ou entité visée à l'article 10 de cette même loi) les renseignements recueillis auprès des transporteurs aériens et des exploitants de systèmes de réservation de services aériens portant sur une personne inscrite ou sur une personne à l'égard de laquelle le ministre de la Sécurité publique et de la Protection civile ou le ministre des Transports a informé l'ASFC qu'il a des raisons de croire qu'il s'agit d'une personne inscrite.

2.7.6 Pouvoir d'exempter (art. 128)

Le nouveau paragraphe 7.1(1) de la LSDA dispose que le ministre de la Sécurité publique et de la Protection civile peut, par arrêté, soustraire un transporteur aérien à son obligation de fournir des renseignements sur les passagers comme le prévoit le nouveau paragraphe 6(2) de la LSDA ou la réglementation lorsqu'il juge :

> a) d'une part, que l'urgence d'une situation ou que des circonstances indépendantes de la volonté du transporteur aérien rendent difficile le fait de se conformer à ce paragraphe ou à cette disposition,
>
> b) d'autre part, que la sûreté des transports ne risque pas d'être compromise.

De plus, le nouvel article 7.2 de la LSDA donne au ministre de la Sécurité publique et de la Protection civile le pouvoir de soustraire un transporteur aérien ou une catégorie de transporteurs aériens à l'application de toute disposition des règlements, afin de permettre « la conduite d'essais, notamment à l'égard de nouvelles technologies ou de procédures de rechange à ce qui est prévu à cette disposition, de façon à permettre au ministre d'établir en conséquence si des changements réglementaires sont nécessaires », « [s]'il est d'avis que la sûreté des transports ne risque pas d'être compromise ».

2.7.7 Destruction des renseignements (art. 136)

En vertu de l'article 136 du projet de loi, l'article 18 de la LSDA est réécrit afin de préciser que nonobstant toute autre loi fédérale, notamment la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*[71], le ministre de la Sécurité publique et de la Protection civile et le ministre des Transports, aux termes des nouveaux paragraphes 18(1) et 18(2) de la LSDA respectivement, sont tous deux tenus de détruire les documents ou registres relatifs à une personne qui est, qui était ou qui devait vraisemblablement être à bord d'un aéronef, dans les sept jours suivant la date de départ ou d'annulation du vol, sauf si ces derniers sont raisonnablement nécessaires pour l'application de la LSDA (renseignements fournis ou communiqués en vertu des par. 6(2) à 6(4) et de l'al. 13d) de la LSDA).

L'article 136 du projet de loi C-59, au nouveau paragraphe 18(3) de la LSDA, dispose aussi que toutes les autres personnes ou entités visées à l'article 10 de la LSDA sont tenues de se conformer à l'exigence relative à la destruction des renseignements. Cela comprend le ministre de la Citoyenneté et de l'Immigration, la GRC, le SCRS, l'ASFC et toute autre personne ou entité prévue par règlement.

En plus de la disposition actuelle prévoyant la collecte, l'utilisation et la communication de l'information, l'article 136 du projet de loi C-59 modifie l'article 19 de la LSDA afin de préciser que la LSDA ne porte aucunement atteinte à la conservation légale de l'information. Autrement dit, le ministère et les organismes fédéraux qui prêtent assistance au ministre de la Sécurité publique et de la Protection civile (en application de l'article 10 de la LSDA), qui sont légalement autorisés à recueillir, utiliser et communiquer des renseignements, peuvent désormais légalement les conserver, si la loi les y autorise.

Par exemple, la LSDA n'entraverait pas la capacité du SCRS de conserver des renseignements qu'il est légalement autorisé à recueillir, utiliser, communiquer ou conserver en vertu de la Loi sur le SCRS. Le cadre d'interprétation prévu à l'article 19 de la LSDA semble refléter la terminologie et le raisonnement qui sous-tendent la décision que la Cour fédérale a rendue en 2016 concernant la conservation de métadonnées par le SCRS, et l'avis de celle-ci que le mandat et les fonctions du SCRS doivent être strictement définis et limités [72].

2.7.8 Recours administratifs (art. 134)

En vertu de la LSDA, une personne inscrite peut demander que son nom soit retiré de la liste dans les 60 jours après s'être vu refuser l'accès à un moyen de transport [73]. Il faut offrir à la personne une occasion raisonnable de présenter des observations. Le ministre de la Sécurité publique et de la Protection civile doit ensuite décider si des motifs raisonnables de garder le nom du demandeur sur la liste existent toujours et, sans délai, informer le demandeur de toute décision (mais pas des motifs de celle-ci) à l'égard de sa demande. Si le ministre ne rend pas de décision sur la demande dans les 90 jours, ou dans toute autre période dont le ministre et le demandeur sont convenus, le ministre est réputé avoir rejetée la demande en question.

Le paragraphe 15(6) modifié de la LSDA accorde au ministre de la Sécurité publique et de la Protection civile 30 jours de plus après le début du délai initial de 90 jours à compter de la date de réception de la demande, ce qui donne un délai total de 120 jours. Si le ministre ne dispose pas de l'information requise pour rendre une décision et qu'il en avise le demandeur dans cette période de 120 jours, le délai peut être prolongé de 120 jours. Contrairement à la présomption établie dans la LSDA, le projet de loi C-59 dit qu'à l'expiration du délai, « le ministre est réputé avoir décidé de radier de la liste le nom du demandeur ». Le Comité SECU a formulé une recommandation semblable [74].

2.7.9 Droit d'appel (art. 135)

La LSDA confère à une personne inscrite le droit d'en appeler devant la Cour fédérale de toute directive ministérielle donnée en vertu de l'article 9 de la LSDA et de toute décision ministérielle d'ajouter ou de garder le nom de la personne sur la liste, rendue en vertu de l'article 8 ou 15 de la LSDA.

Une personne inscrite ayant fait l'objet d'un refus de transport en raison d'une directive donnée en vertu de l'article 9 de la LSDA peut interjeter appel seulement après s'être vu refuser le retrait de son nom de la liste des personnes précisées à la suite du recours administratif prévu à l'article 15 de la LSDA. L'article 16 de la LSDA dispose qu'une période d'appel de 60 jours s'applique.

L'article 135 du projet de loi C-59 modifie le paragraphe 16(2) de la LSDA afin de tenir compte des modifications apportées aux dispositions relatives aux recours administratifs et de la suppression du renvoi à la décision présumée du ministre de la Sécurité publique et de la Protection civile en vertu du paragraphe 15(6) de la LSDA. Un appel peut être interjeté dans les 60 jours suivant la réception de l'avis de la décision du ministre dont il est question dans l'actuel paragraphe 15(5) de la LSDA. Le projet de loi n'élimine pas le droit d'appel d'une directive donnée en vertu de l'article 9 de la LSDA ni de toute décision rendue par le ministre en vertu de l'article 15 de la LSDA.

Il convient de souligner que le projet de loi C-59 ne modifie pas les procédures d'appel en vigueur dans la LSDA. Ces dernières sont très similaires à celles prévues dans la *Loi sur l'immigration et la protection des réfugiés* (LIPR) d'avant 2008 pour le contrôle des certificats de sécurité et des ordonnances de détention. Dans l'arrêt *Charkaoui c. Canada (Citoyenneté et Immigration)*, la Cour suprême du Canada a examiné ce processus et déterminé que le régime de la LIPR portait atteinte au droit à la vie, à la liberté et à la sécurité de la personne, en précisant qu'il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale garantis par l'article 7 de la *Charte*[75].

Même si une personne inscrite sur la LPP peut présenter une demande de radiation au juge en chef de la Cour fédérale[76], elle n'aura pas accès aux documents confidentiels, et la LSDA – contrairement à la procédure prévue à l'égard des certificats de sécurité dans la *Loi sur l'immigration et la protection des réfugiés* – ne prévoit pas le recours à un avocat spécial[77].

Lors de tels appels, la Cour fédérale doit déterminer si la décision est raisonnable compte tenu de l'information dont elle dispose. Comme le prévoit l'alinéa 16(6)e) de la LSDA, les règles de preuve habituelles ne s'appliquent pas à l'instance d'appel, étant donné que la LSDA permet l'admission d'une preuve par ouï-dire : « [le juge] peut recevoir et admettre en preuve tout élément – même inadmissible en justice – qu'il estime digne de foi et utile et peut fonder sa décision sur celui-ci ». Aux termes des alinéas 16(6)a) à 16(6)c) de la LSDA :

> a) à tout moment pendant l'instance et à la demande du ministre, le juge doit tenir une audience à huis clos et en l'absence de l'appelant et de son conseil dans le cas où la divulgation des renseignements ou autres éléments de preuve en cause pourrait porter atteinte, selon lui, à la sécurité nationale ou à la sécurité d'autrui;
> b) il lui incombe de garantir la confidentialité des renseignements et autres éléments de preuve que lui fournit le ministre et dont la divulgation porterait atteinte, selon lui, à la sécurité nationale ou à la sécurité d'autrui;
> c) il veille tout au long de l'instance à ce que soit fourni à l'appelant un résumé de la preuve qui ne comporte aucun élément dont la divulgation porterait atteinte, selon lui, à la sécurité nationale ou à la sécurité d'autrui et qui permet à l'appelant d'être suffisamment informé de la thèse du ministre à l'égard de l'instance en cause.

En définitive, le juge peut fonder sa décision sur des renseignements et autres éléments de preuve même si un résumé de ces derniers n'est pas fourni à l'appelant.

Dans son rapport *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale du Canada*, le Comité SECU a recommandé que la LSDA soit modifiée dans le but de prévoir la nomination d'un avocat spécial pour protéger les intérêts des personnes qui ont interjeté appel afin de faire retirer leur nom de la LPP. Le Comité SECU a fait état de l'étendue des atteintes à la liberté et à la sécurité des personnes par suite de l'application des dispositions d'appel et réclamé plus d'équité, d'ouverture et de transparence. En outre, le Comité SECU a recommandé que le rapport annuel de Sécurité publique Canada au Parlement précise le nombre de personnes inscrites sur la LPP [78]. Le projet de loi C-59 ne donne pas suite à ces recommandations.

2.8 PARTIE 7 : MODIFICATIONS DU *CODE CRIMINEL* (ART. 140 À 154)

2.8.1 Contexte

Dans le cadre des consultations sur la sécurité nationale, le gouvernement du Canada s'est penché, dans son document intitulé *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016*, sur les mesures de lutte contre le terrorisme prévues au *Code criminel*. Le document explique que le projet de loi C-51, c'est-à-dire la *Loi antiterroriste de 2015*, avait modifié le *Code criminel* afin de :

> a) faire en sorte qu'il soit plus facile d'empêcher l'exécution d'activités terroristes ou d'infractions de terrorisme;
> b) rendre criminel le fait de préconiser ou de fomenter des infractions de terrorisme;
> c) donner aux tribunaux le pouvoir d'ordonner la saisie ou la confiscation de propagande terroriste;
> d) accorder une protection supplémentaire aux témoins et aux autres participants dans les instances relatives à la sécurité nationale [79].

Le rapport sur les résultats des consultations intitulé *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*, publié en mars 2017, disait ceci sur le *Code criminel* :

- la plupart des participants ont dit craindre que les modifications apportées au *Code criminel* en réponse à l'entrée en vigueur de la *Loi antiterroriste de 2015* « puissent entraîner une perte de libertés personnelles et porter atteinte à la liberté d'expression [80] »;
- les deux tiers des participants ont affirmé que « les seuils d'application mis en place pour obtenir un engagement assorti de conditions et un engagement de ne pas troubler l'ordre public lié au terrorisme » sont inappropriés et ne constituent pas « un juste équilibre entre la sécurité nationale et la protection des droits des personnes [81] »;
- « [p]rès de la moitié (47 %) des réponses en ligne indiquent que l'infraction consistant à préconiser des actes de terrorisme devrait être clarifiée afin qu'elle ressemble plus clairement à l'infraction actuelle qui consiste à "conseiller" la perpétration de tels actes [82] »;
- la plupart des participants sont d'avis que la définition de « propagande terroriste » « est maintenant trop large et pourrait entraîner une déclaration de culpabilité pour des personnes innocentes [83] ».

Le Livre vert du gouvernement traitait aussi des procédures d'inscription à la liste des entités terroristes, prévues au *Code criminel*. À cet égard, le document *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris* précise que 52 % des répondants étaient d'avis que « les méthodes d'inscription actuelles répondent aux besoins nationaux et aux obligations internationales du Canada [84] », et que 44 % étaient d'avis « que ce n'était pas le cas ». Selon 62 % des répondants :

> les mesures de protection actuelles n'offrent pas un équilibre adéquat entre la sécurité nationale et la protection des droits des Canadiens, et plusieurs suggestions sont formulées pour améliorer les mesures de protection : clarifier la définition de « terrorisme » et les critères relatifs à l'ajout d'un groupe ou d'un individu sur la liste, rendre la liste publique, créer un processus d'appel et imposer une surveillance plus indépendante [85].

Dans son rapport de 2017 intitulé *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale du Canada*, le Comité SECU a formulé des recommandations pour réformer les mesures de lutte contre le terrorisme prévues au *Code criminel* [86].

2.8.2 Régime d'inscription des entités terroristes prévu par l'article 83.05 du *Code criminel*

2.8.2.1 Régime actuel

En 2001, la *Loi antiterroriste* a édicté de nouvelles dispositions du *Code criminel* prévoyant un régime d'inscription d'entités impliquées dans des activités terroristes [87]. Le *Code criminel* établit la procédure applicable d'inscription et de radiation des entités sur la liste. Le terme « entité » est ainsi défini : « Personne, groupe, fiducie, société de personnes ou fonds, ou organisation ou association non dotée de la personnalité morale [88] ».

De manière générale, le gouverneur en conseil est autorisé à établir une liste par règlement [89]. En vertu du paragraphe 83.05(1) du *Code criminel*, le gouverneur en conseil peut inscrire sur la liste :

> toute entité dont il est convaincu, sur la recommandation du ministre de la Sécurité publique et de la Protection civile, qu'il existe des motifs raisonnables de croire :
>
> a) que, sciemment, elle s'est livrée ou a tenté de se livrer à une activité terroriste, y a participé ou l'a facilitée;
>
> b) que, sciemment, elle a agi au nom d'une entité visée à l'alinéa a), sous sa direction ou en collaboration avec elle.

Les principales conséquences du régime d'inscriptions d'entités impliquées dans des activités terroristes sont les suivantes :

- Bien que l'« inscription d'une entité sur la liste ne signifie pas que celle-ci a commis un crime », cela constitue « un moyen public d'indiquer qu'un groupe ou un particulier est associé au terrorisme[90] ».
- Une entité inscrite sur la liste est automatiquement considérée comme étant un « groupe terroriste » au sens du *Code criminel*. En fait, il est important de noter que la définition de « groupe terroriste » au paragraphe 83.01(1) du *Code criminel* englobe les entités inscrites sur la liste établie par le gouverneur en conseil en vertu de l'article 83.05 du *Code criminel*. Le terme « groupe terroriste » est utilisé à de multiples endroits dans le *Code criminel*, notamment pour établir des infractions liées au terrorisme (voir, par exemple, l'article 83.18 du *Code criminel* concernant la participation à une activité d'un groupe terroriste). Bref, lorsqu'une entité est inscrite sur la liste, la preuve n'a pas à être faite que l'un de ses objets ou l'une de ses activités est de se livrer à des activités terroristes ou de les faciliter[91].
- Les entités inscrites sur la liste peuvent voir leurs biens saisis, bloqués ou confisqués conformément aux articles 83.08 et suivants du *Code criminel*[92]. Comme le précise Sécurité publique Canada, en vertu de l'article 83.11 du *Code criminel*, certaines institutions, comme les banques, « ont l'obligation de soumettre des rapports concernant les avoirs d'une entité et d'empêcher l'entité d'accéder à ces avoirs[93] ».

2.8.2.2 Modifications de la procédure d'inscription et de radiation des entités impliquées dans des activités terroristes (art. 141 et 142)

L'article 141 du projet de loi C-59 modifie certaines règles prévues au *Code criminel* relativement au régime d'inscription d'entités impliquées dans des activités terroristes.

Selon le nouvel alinéa 83.05(1.2)a) du *Code criminel*, ajouté au paragraphe 141(2) du projet de loi, s'il a des motifs raisonnables de croire qu'une entité inscrite utilise un nom ne figurant pas sur la liste, le ministre de la Sécurité publique et de la Protection civile peut :

- modifier le nom d'une entité qui figure sur la liste;
- ajouter à la liste tout autre nom.

Il semble que cette nouvelle disposition allège le fardeau de la preuve en ce qui concerne l'ajout du nom d'une entité liée à une entité déjà inscrite sur la liste, étant donné qu'à l'heure actuelle, comme précisé précédemment, une entité peut être inscrite sur la liste en vertu du paragraphe 83.05(1) du *Code criminel*, s'il existe des motifs raisonnables de croire « que, sciemment, elle s'est livrée ou a tenté de se livrer à une activité terroriste, y a participé ou l'a facilitée » ou « que, sciemment, elle a agi au nom d'une entité visée […], sous sa direction ou en collaboration avec elle ».

De même, aux termes du nouvel alinéa 83.05(1.2)b) du *Code criminel*, le ministre est autorisé à radier de la liste un nom sous lequel une entité inscrite peut aussi avoir été connue, si l'entité n'utilise plus ce nom.

En vertu du paragraphe 83.05(3) du *Code criminel*, le délai pour rendre une décision relativement à une demande de radiation présentée par une entité inscrite passe de 60 à 90 jours. Si le ministre n'a pas rendu de décision à l'intérieur de ce délai (ou dans un délai plus long convenu entre le ministre et le demandeur), le ministre est réputé avoir décidé que le demandeur devrait rester inscrit sur la liste.

L'article 141 du projet de loi modifie les règles régissant l'examen périodique de la liste par le ministre afin de déterminer si l'inscription d'une entité sur la liste est toujours justifiée. Le nouveau paragraphe 83.05(8.1) du *Code criminel* prévoit l'examen quinquennal des entités inscrites sur la liste. À l'heure actuelle, la période d'examen est de deux ans (par. 83.05(9) du *Code criminel*). En vertu du nouveau paragraphe 83.05(10), le ministre doit faire publier dans la *Gazette du Canada* un avis portant sur les résultats de l'examen d'une entité inscrite effectué dans les cinq ans suivant la conclusion de l'examen. Pour l'heure, le paragraphe 83.05(10) du *Code criminel* prévoit que les résultats de cet examen doivent être publiés sans délai dans la *Gazette du Canada*.

2.8.3 Conseiller la commission d'une infraction de terrorisme (art. 143)

La *Loi antiterroriste de 2015* (ancien projet de loi C-51) a créé l'article 83.221 du *Code criminel*, qui porte sur le fait de préconiser ou de fomenter la perpétration d'infractions de terrorisme en général.

Lors de sa comparution devant le Comité SECU, en mars 2015, dans le cadre de l'étude du projet de loi C-51, l'honorable Peter MacKay, alors ministre de la Justice et procureur général du Canada, a expliqué que le nouvel article 83.221 comblait une lacune :

> Actuellement, il est illégal de conseiller à quelqu'un de commettre un crime précis, comme un meurtre. Toutefois, il n'est pas illégal de conseiller à quelqu'un de commettre un large éventail d'activités criminelles, comme le terrorisme, en l'absence de détails précis quant à l'infraction que la personne est encouragée à commettre. Par conséquent, la nouvelle infraction proposée vise à tenir compte des cas où l'incitation active ne comporte pas de détail précis qui permettrait d'établir un lien entre l'encouragement et la commission d'une infraction précise de terrorisme, même si dans les circonstances, il est clair que l'on encourage activement une personne à commettre les infractions de terrorisme prévues dans le *Code criminel*. Autrement dit, il importerait peu qu'une infraction précise de terrorisme soit préconisée ou fomentée pour que la responsabilité criminelle y soit rattachée. Pour être clair, il ne s'agit pas d'une infraction liée à la glorification du terrorisme[94].

Il est à noter que le rapport du Comité SECU sur le cadre de la sécurité nationale déposé en mai 2017 indique que la portée de l'article 83.221 du *Code criminel* est critiquée. Selon un certain nombre de témoins,

> cette nouvelle infraction serait anticonstitutionnelle, parce qu'elle est vague, trop large et qu'elle restreindrait de manière déraisonnable la liberté d'expression […] Pour qu'une telle infraction puisse être justifiée, il doit exister un lien étroit entre la déclaration qui est communiquée et le risque de préjudice [95].

L'article 143 du projet de loi modifie l'article 83.221 du *Code criminel*. Les modifications sont présentées dans le tableau 1 ci-dessous.

Tableau 1 – Modifications apportées à l'article 83.221 du *Code criminel* prévues dans le projet de loi C-59 (Préconiser ou fomenter la commission d'infractions de terrorisme)

Article 83.221 actuellement en vigueur	Article 83.221 du projet de loi C-59
83.221(1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans, quiconque, sciemment, par la communication de déclarations, préconise ou fomente la perpétration d'infractions de terrorisme en général – exception faite de l'infraction visée au présent article –, sachant que la communication entraînera la perpétration de l'une de ces infractions ou sans se soucier du fait que la communication puisse ou non entraîner la perpétration de l'une de ces infractions. (2) Les définitions qui suivent s'appliquent au présent article. *communiquer* S'entend au sens du paragraphe 319(7). *déclarations* S'entend au sens du paragraphe 319(7).	83.221(1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans, quiconque conseille à une autre personne de commettre une infraction de terrorisme sans préciser laquelle. (2) Pour que l'infraction prévue au paragraphe (1) soit commise, il n'est pas nécessaire que l'infraction de terrorisme soit commise par la personne qui a été conseillée.

Les termes utilisés actuellement à l'article 83.221 du *Code criminel* – « par la communication de déclarations, préconise ou fomente la perpétration d'infractions de terrorisme en général » – sont similaires à ceux utilisés aux articles 318 et 319 du *Code criminel* pour établir les infractions liées à la propagande haineuse. Il est à noter que des moyens de défense précis sont prévus au paragraphe 319(3) du *Code criminel* pour l'infraction consistant à fomenter volontairement la haine, prévue au paragraphe 319(2) du *Code criminel*. Néanmoins, de tels moyens de défense ne sont pas prévus à l'article 83.221 du *Code criminel*. D'ailleurs, certains témoins qui ont comparu devant le Comité SECU dans le cadre de son étude sur le cadre de sécurité nationale :

> se sont demandé pourquoi la nouvelle infraction n'inclut pas des moyens de défense semblables à ceux prévus à l'égard de l'infraction consistant à fomenter la haine […], ou tout simplement pourquoi d'autres infractions – comme celle consistant à inciter quelqu'un à participer à une activité d'un groupe terroriste ou à charger une personne de se livrer à une activité terroriste […] – ne sont pas suffisantes [96].

En outre, les termes utilisés dans le nouvel article 83.221 – « conseille à une autre personne de commettre une infraction de terrorisme » – sont similaires à ceux utilisés pour l'infraction en matière de conseil prévue à l'article 22 du *Code criminel*. Néanmoins, le *Code criminel* ne prévoit aucun moyen de défense spécifique à l'infraction consistant à conseiller la commission d'une telle infraction.

Enfin, dans sa forme actuelle, l'article 83.221 du *Code criminel* érige en infraction le fait de préconiser ou de fomenter la perpétration « d'infractions de terrorisme en général » par la communication de déclarations. Le nouvel article 83.221 du *Code criminel* érige en infraction le fait de conseiller à une autre personne de commettre « une infraction de terrorisme sans préciser laquelle ». La distinction réelle entre les deux descriptions n'est pas claire.

2.8.4 Propagande terroriste (art. 144)

Le *Code criminel* prévoit la délivrance de mandats pour saisir et confisquer des publications ou pour effacer d'un ordinateur toutes données électroniques qui constituent de la « propagande terroriste ».

L'article 144 du projet de loi modifie la définition de « propagande terroriste » prévue au paragraphe 83.222(8) du *Code criminel* de manière à l'accorder avec le langage employé pour décrire la nouvelle infraction consistant à conseiller la commission d'une infraction de terrorisme.

2.8.5 Mesures préventives

À l'heure actuelle, le *Code criminel* prévoit diverses mesures pour prévenir la commission d'actes terroristes :

- investigations devant un juge (art. 83.28 et 83.29);
- arrestation préventive sans mandat et détention d'une semaine maximum (par. 83.3(4));
- engagement assorti de conditions (par. 83.3(8));
- engagements de ne pas troubler l'ordre public lorsqu'une personne a des motifs raisonnables de craindre la possibilité qu'une autre personne commette une infraction de terrorisme (art. 810.011).

Ces mesures attirent souvent la critique.

2.8.5.1 Investigations (art. 145 et 147)

Le projet de loi C-59 supprime les investigations devant un juge. Mis à part le cas de l'enquête dans l'affaire Air India [97], cette procédure spéciale n'a jamais été utilisée.

2.8.5.2 Arrestation sans mandat et engagement assorti de conditions (art. 146 et 148)

Un engagement assorti de conditions peut être utilisé lorsque la police soupçonne un lien quelconque entre une personne et l'exécution d'une activité terroriste. Par exemple, si la GRC soupçonne une personne d'être associée à un vaste complot d'attentat dans une gare ferroviaire, mais qu'elle ne connaît pas le rôle exact de cette personne, elle peut utiliser un engagement de ne pas troubler l'ordre public pour empêcher la personne de commettre une infraction de terrorisme précise, comme utiliser des explosifs ou tenter de quitter le Canada pour rejoindre un groupe terroriste.

Le projet de loi C-59, en vertu du nouvel alinéa 83.3(2)b) et du nouveau paragraphe 83.3(4) du *Code criminel*, resserre les conditions auxquelles une personne soupçonnée de terrorisme peut être arrêtée sans mandat et un engagement assorti de conditions peut être obtenu, comme le prévoit l'article 83.3 du *Code criminel*. Ces conditions avaient été assouplies dans la *Loi antiterroriste de 2015* afin de faciliter le recours à ces procédures d'exception pour la police.

Le nouveau paragraphe 83.32(1) du *Code criminel* prolonge la période de validité de l'article 83.3 à cinq ans après l'entrée en vigueur du projet de loi C-59. En vertu des règles actuelles, cet article était censé être abrogé automatiquement le 15e jour de séance suivant le 15 juillet 2018, à moins que le Parlement, après avoir effectué un examen approfondi, ait adopté une résolution autorisant sa prolongation.

Notons que depuis la création de ces mesures en 2001, la police n'a eu recours ni à l'arrestation sans mandat ni à l'engagement assorti de conditions.

2.8.5.3 Engagements de ne pas troubler l'ordre public (art. 153)

Le nouveau paragraphe 810.011(15) du *Code criminel* exige du procureur général du Canada qu'il produise un rapport sur le nombre d'engagements contractés annuellement en vertu de l'article 810.011.

Il convient de noter que la police a recours fréquemment à l'engagement de ne pas troubler l'ordre public prévu à l'article 810.011 du *Code criminel* et que c'est sans doute la raison pour laquelle le projet de loi C-59 comprend une disposition de surveillance de ce type d'engagement.

2.8.6 Protection des témoins (art. 154)

Une autre question soulevée régulièrement dans le cadre des procès pour terrorisme concerne la protection des témoins.

L'article 486 et les dispositions suivantes du *Code criminel* prévoient des règles régissant la protection des témoins. À titre d'exemple, l'article 486 permet au tribunal d'ordonner que soit exclu de la salle d'audience l'ensemble ou tout membre du public ou autoriser une personne à témoigner derrière un écran, et l'article 486.7 du *Code criminel* permet au tribunal, sur demande du poursuivant, d'autoriser une personne à témoigner de façon anonyme.

Le nouvel article 810.5 du *Code criminel* autorise le tribunal à rendre les ordonnances de protection des témoins prévues aux articles 486 à 486.5 et 486.7 du *Code criminel* aux fins des procédures engagées aux articles 83.3 et 810 à 810.2.

2.9 PARTIE 8 : MODIFICATIONS DE LA *LOI SUR LE SYSTÈME DE JUSTICE PÉNALE POUR LES ADOLESCENTS* (ART. 159 À 167)

La *Loi sur le système de justice pénale pour les adolescents* [98] (LSJPA), entrée en vigueur en 2003, établit un système de justice pénale distinct de celui s'appliquant aux adultes et fondé sur le principe selon lequel le degré de culpabilité morale est moins élevé pour les jeunes que pour les adultes. La LSJPA s'applique lorsqu'un jeune âgé de 12 à 17 ans est impliqué dans une infraction créée par une loi fédérale (tel que le *Code criminel*) et son règlement d'application. La LSJPA porte également création du tribunal pour adolescents.

2.9.1 Application des mesures de protection pour les adolescents (art. 159 à 164)

La LSJPA dit que le système de justice pénale pour les adolescents a comme objectif la protection du public « au moyen de mesures proportionnées à la gravité de l'infraction et au degré de responsabilité » des adolescents, tout en prévoyant des règles spéciales visant à garantir leurs droits et libertés [99].

Le nouveau paragraphe 14(2) de la LSJPA, prévu à l'article 159 du projet de loi, précise expressément que les principes et garanties de la LSJPA s'appliquent aux mesures préventives de lutte contre le terrorisme établies aux articles 83.3 et 810.011 du *Code criminel*. Le nouveau paragraphe 29(1) de la LSJPA, à l'article 163 du projet de loi, indique que le principe selon lequel la détention ne doit pas se substituer à des mesures sociales (par exemple, de santé mentale ou de protection de la jeunesse) s'applique à la détention préventive prévue à l'article 83.3 du *Code criminel*. Le nouveau paragraphe 30(1) de la LSJPA, prévu à l'article 164 du projet de loi, dispose que les jeunes doivent être détenus dans des conditions qui sont sécuritaires, justes et humaines.

Les nouveaux alinéas 25(3)a) et 25(3)a.1) de la LSJPA, à l'article 161 du projet de loi, disposent que le tribunal pour adolescents est tenu d'informer les adolescents de leur droit aux services d'un avocat lorsqu'ils font l'objet de mesures préventives de lutte contre le terrorisme.

2.9.2 Accès aux dossiers des adolescents pour l'application du *Décret sur les passeports canadiens* (art. 167)

L'alinéa 3(1)b) de la LSJPA prévoit que « le système de justice pénale pour les adolescents doit être distinct de celui pour les adultes, être fondé sur le principe de culpabilité morale moins élevée et mettre l'accent sur », notamment, « la prise de mesures procédurales supplémentaires pour leur assurer un traitement équitable et la protection de leurs droits, notamment en ce qui touche leur vie privée ». En effet, depuis la *Loi sur les jeunes délinquants* de 1908 :

> le système de justice des mineurs canadiens repose sur le principe que la publication de l'identité de l'adolescent nuirait à sa réinsertion sociale, lui causerait un préjudice et, par le fait même, compromettrait la sécurité du public à long terme [100].

La règle générale veut donc, en vertu de l'article 110 de la LSJPA, que les enseignements relatifs à l'identité de l'adolescent ne soient pas publiés. Les règles relatives à la tenue de dossiers par les tribunaux, la police et les ministères ou organismes canadiens sont prévues aux articles 114 à 116 de la LSJPA. L'article 117 et les dispositions suivantes de la LSJPA prévoient aussi des règles restreignant l'accès aux dossiers des adolescents. En général, comme le prévoit l'article 118 de cette même loi, l'accès aux dossiers des adolescents est interdit.

Plus précisément, l'article 119 de la LSJPA désigne les personnes – comme les parents, les victimes, les juges et les procureurs – qui peuvent avoir accès au dossier d'un adolescent. De plus, cet article prévoit un délai précis pour l'accès à certains renseignements d'un dossier. À l'expiration de ce délai, l'accès au dossier n'est plus autorisé.

Le paragraphe 167(1) du projet de loi C-59 ajoute un nouvel alinéa au paragraphe 119(1) de la LSJPA de manière à ce que « tout employé d'un ministère ou organisme fédéral, pour l'application du *Décret sur les passeports canadiens* » fasse partie des « personnes ayant accès aux dossiers » en vertu de la LSJPA. Le *Décret sur les passeports canadiens* vise la délivrance des passeports, le refus de délivrance, la révocation ainsi que l'annulation de passeports [101].

Actuellement, le paragraphe 119(2) de la LSJPA ne prévoit pas de période d'accès aux dossiers d'adolescents visés par des ordonnances prises en vertu du paragraphe 14(2) de la LSJPA (telles que des ordonnances concernant un engagement lié à des activités terroristes [art. 83.3 du *Code criminel*]) et en vertu du

paragraphe 20(2) de la LSJPA (engagement – crainte de blessures ou dommages [art. 810 du *Code criminel*]). Le paragraphe 167(2) du projet de loi C-59, en vertu du nouvel alinéa 119(2)d.1) de la LSJPA, restreint à six mois l'accès aux dossiers des adolescents visés par une ordonnance prise en vertu des paragraphes 14(2) et 20(2) de la LSJPA.

NOTES

1. Projet de loi C-59, Loi concernant des questions de sécurité nationale, 1re session, 42e législature.
2. Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada, 1977-1981.
3. Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, *Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale*, 2006; et Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, *Commission Arar – Enquête sur les faits*.
4. Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin, *Rapport final*.
5. Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India, *Vol 182 d'Air India : Une tragédie canadienne*, rapport final, 2010.
6. Projet de loi C-51, Loi édictant la Loi sur la communication d'information ayant trait à la sécurité du Canada et la Loi sur la sûreté des déplacements aériens, modifiant le Code criminel, la Loi sur le Service canadien du renseignement de sécurité et la Loi sur l'immigration et la protection des réfugiés et apportant des modifications connexes et corrélatives à d'autres lois, 2e session, 41e législature (L.C. 2015, ch. 20) (Loi antiterroriste de 2015). Voir aussi Julie Béchard *et al.*, *Résumé législatif du projet de loi C-51 : Loi édictant la Loi sur la communication d'information ayant trait à la sécurité du Canada et la Loi sur la sûreté des déplacements aériens, modifiant le Code criminel, la Loi sur le Service canadien du renseignement de sécurité et la Loi sur l'immigration et la protection des réfugiés et apportant des modifications connexes et corrélatives à d'autres lois*, publication nº 41-2-C51-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 19 juin 2015.
7. Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016*, 2016.
8. Hill et Knowlton Stratégies, *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*.
9. *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, L.C. 2017, ch. 15. Voir aussi Holly Porteous et Dominique Valiquet, *Résumé législatif du projet de loi C-22 : Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement et modifiant certaines lois en conséquence*, publication nº 42-1-C22-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 22 août 2016.
10. Voir le résumé des témoignages reçus dans le cadre de l'étude et du rapport du Comité permanent de la sécurité publique et nationale (SECU) de la Chambre des communes, *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale du Canada*, neuvième rapport, 1re session, 42e législature, mai 2017.
11. *Loi sur la protection de l'information*, L.R.C. 1985, ch. O-5.
12. Cela dit, en vertu du principe du « droit de regard de la source », des pays alliés pourraient exercer leur droit de bloquer l'accès de l'OSASNR à l'information. Les mises en garde contre la communication de renseignements à des tiers sans le consentement de la source constituent une forme de droit de regard de la source. Voir la mention « droit de regard de la source » à l'art. 117 du projet de loi, lequel modifie l'art. 4 de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*.
13. *Loi sur la défense nationale*, L.R.C. 1985, ch. N-5.
14. *Loi sur les enquêtes*, L.R.C. 1985, ch. I-11.
15. *Loi sur la Gendarmerie royale du Canada*, L.R.C. 1985, ch. R-10.
16. *Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21.

17. *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, L.C. 2000, ch. 17.

18. Les dispositions de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*, établies dans la partie 5 du projet de loi C-59, sont abordées à la section 2.6 du présent résumé législatif.

19. *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23.

20. *Loi sur la gestion des finances publiques*, L.C. 1985, ch. F-11.

21. *Loi sur l'emploi dans la fonction publique*, L.C. 2003, ch. 22, art. 12 et 13.

22. Cette formulation englobe les cours supérieures et les cours d'appel de chaque province, mais exclut la Cour suprême du Canada, la Cour fédérale, la Cour d'appel fédérale et les cours provinciales.

23. Ministère de la Justice, *Énoncé concernant la Charte – Projet de loi C-59 : la* Loi concernant des questions de sécurité nationale, 20 juin 2017.

24. Les décisions du commissaire au renseignement seraient vraisemblablement assujetties à un processus de contrôle judiciaire en vertu de la *Loi sur les Cours fédérales*. Les pouvoirs de contrôle judiciaire de la Cour fédérale s'appliquent à tout office fédéral, à savoir :

> 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, à l'exclusion de la Cour canadienne de l'impôt et ses juges, d'un organisme constitué sous le régime d'une loi provinciale ou d'une personne ou d'un groupe de personnes nommées aux termes d'une loi provinciale ou de l'article 96 de la *Loi constitutionnelle de 1867*.

Voir *Loi sur les Cours fédérales*, L.R.C. 1985, ch. F-7, par. 2(1).

25. L'art. 4 de la Loi sur le Centre de la sécurité des télécommunications soulève la possibilité qu'un autre ministre soit désigné pour assumer la responsabilité du CST.

26. Il convient de souligner qu'en vertu de la Loi sur le CST proposée (dont il est question à la section 2.4 du présent résumé législatif), le CST sera habilité à se livrer à cinq catégories d'activités, dont chacune nécessitera une autorisation ministérielle. Toutefois, seules les activités de collecte de renseignements étrangers et de cybersécurité nécessiteront l'approbation du commissaire au renseignement.

27. Voir les art. 26, 27 et 29 de la Loi sur le CST, à l'art. 76 du projet de loi C-59.

28. Les logiciels de reconnaissance faciale sont de plus en plus utilisés pour le contrôle frontalier et la lutte contre le terrorisme.

29. Par exemple, Internet est conçu pour assurer la redondance et l'adaptabilité en cas de pannes localisées ou de pointes de trafic. Ainsi, une communication transmise par Internet peut un jour passer par un ensemble de routeurs et le lendemain, par un ensemble de routeurs complètement différents.

30. Par exemple, le CST pourrait devoir acquérir de l'information de cette manière afin de savoir et de caractériser comment ses cibles de renseignement étranger interagissent avec l'infrastructure mondiale de l'information.

31. *Code criminel*, L.R.C. 1985, ch. C-46.

32. Voir Jordan Press, La Presse Canadienne, « Top courts threaten federal government with legal action over new IT rules », *Globe and Mail*, 16 mai 2018. Voir aussi Amanda Connolly, « CSE chief says federal departments need to 'get on' Shared Services' cyber defences », *iPolitics*, 21 mars 2016.

33. Des observateurs ont laissé entendre que le CST pourrait « utiliser des agents humains pour modifier des logiciels, implanter des dispositifs matériels ou autrement faciliter la collecte de renseignements étrangers » [TRADUCTION]. Voir Bill Robinson, « CSE and Bill C-59 Overview », *Lux Ex Umbra*, blogue, 4 août 2017.

34. *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, ch. 11.

35. En activité depuis décembre 2016, l'Échange canadien de menaces cybernétiques est un organisme sans but lucratif qui, moyennant des frais d'adhésion annuels de 50 000 $, offre aux propriétaires et exploitants d'infrastructures essentielles un accès aux renseignements partagés sur les cybermenaces, notamment l'information expurgée du CST. Dans le vocabulaire du renseignement, l'information expurgée est celle dont la communication a été approuvée après nettoyage. Par exemple, avant de communiquer au secteur privé des données du renseignement sur des menaces, le CST aura probablement supprimé toute information révélant les sources et les méthodes utilisées pour obtenir le renseignement. Cette opération peut être réalisée avec des moyens automatisés. Pour en savoir plus, voir « The Canadian Cyber Threat Exchange (CCTX) is operational and reaching out to Canadian businesses », *Canadian News Wire*, 9 décembre 2016; et Échange canadien de menaces cybernétiques, *Frequently Asked Questions*.

36. L'al. 34(2)c) de la Loi sur le CST dispose que :

> (2) Le ministre ne peut délivrer l'autorisation visée au paragraphe 26(1) [autorisation de renseignement étranger] que s'il conclut qu'il y a des motifs raisonnables de croire, outre ce qui est prévu au paragraphe (1) :
>
> > c) que les mesures visées à l'article 24 permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle aux affaires internationales, à la défense ou à la sécurité.

L'Énoncé concernant la *Charte* du projet de loi C-59 dit ceci relativement à l'art. 33 :

> De plus, aucune activité visant des Canadiens ou des personnes au Canada ne pourrait être autorisée; seules les activités visant des étrangers et l'[infrastructure mondiale d'information (IMI)] qui ne sont pas situés au Canada pourraient être autorisées.

Voir ministère de la Justice (2017).

37. Aux termes de l'art. 2 du *Code criminel*, s'entend de « lésions corporelles » toute « [b]lessure qui nuit à la santé ou au bien-être d'une personne et qui n'est pas de nature passagère ou sans importance ».

38. Voir, par exemple, Bureau du commissaire du CST, « Modifications proposées à la *Loi sur la défense nationale* », *Rapport annuel 2007-2008*, 2008, p. 4; Bureau du commissaire du CST, « Examen des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers (volet 2) », *Rapport annuel 2015-2016*, 2016, p. 21 à 24. Voir aussi Commissariat à la protection de la vie privée du Canada, recommandation 9 dans « Améliorations recommandées », *Rapport spécial au Parlement – Mesures de vérification et de contrôle : Renforcer la protection de la vie privée et la supervision des activités du secteur canadien du renseignement à l'ère de la cybersurveillance*, 28 janvier 2014; et Commissariat à la protection de la vie privée du Canada, *La protection de la vie privée et le cadre de sécurité nationale du Canada*, document d'information, 6 décembre 2016.

39. Owen Bowcott, « UK intelligence agencies face surveillance claims in European court », *The Guardian* [Londres], 7 novembre 2017 [TRADUCTION].

40. Royaume-Uni, Investigatory Powers Tribunal, *Privacy International vs. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service*, [2016] UKIPTrib 15_110-CH, par. 7(48) [TRADUCTION].

41. Ministère de la Justice (2017).

42. Les juristes qualifient ce type de disposition de « clause Henry VIII » en référence à la loi sur les proclamations de 1539, qui a conféré au roi Henry VIII le pouvoir de légiférer par proclamation. Au Royaume-Uni, la commission Donoughmore sur les pouvoirs des ministres a indiqué que cette pratique était « incompatible avec les usages d'un régime parlementaire, où l'autorité législative supérieure confère à l'autorité législative subordonnée le pouvoir de modifier une loi ayant été adoptée par l'autorité législative supérieure » [TRADUCTION] (cité dans Helen Xanthaki, *Thornton's Legislative Drafting*, 5e éd., Bloomsbury Professional, Londres, 2013, p. 420). Toutefois, une clause Henry VIII se justifie dans certains cas, comme lorsque le pouvoir délégué est limité et utilisé seulement pour garantir que la législation subordonnée respecte toujours les principes de la législation principale. Pour en savoir plus sur les clauses Henry VIII, voir Stephen Argument, *Henry VIII clauses: Fact sheet*, Standing Committee on Justice and Community Safety (performing the duties of a Scrutiny of Bills and Subordinate Legislation Committee), Assemblée législative du Territoire de la capitale de l'Australie, novembre 2011.

    Bien que la jurisprudence donne à penser que de telles clauses sont constitutionnelles, il convient de souligner que l'affaire principale citée – *In Re George Edwin Gray*, 57 SCR 150, 1918 CanLII 533 (SCC) [DISPONIBLE EN ANGLAIS SEULEMENT] – renvoie à la délégation de pouvoirs par le Parlement au gouverneur en conseil en vertu de la *Loi sur les mesures de guerre* de 1914 afin d'autoriser :

> tels actes et choses et de faire de temps à autre tels ordres et règlements qu'il peut, à raison de l'existence réelle ou appréhendée de la guerre, d'une invasion ou insurrection, juger nécessaires ou à propos pour la sécurité, la défense, la paix, l'ordre et le bien-être du Canada.

43. *Loi sur la responsabilité civile de l'État et le contentieux administratif*, L.R.C. 1985, ch. C-50.

44. *X (Re)*, 2016 CF 1105.

45. *Ibid*., par. 255 à 257.

46. Les institutions fédérales, dont le Service canadien du renseignement de sécurité (SCRS), doivent se conformer à la *Loi sur la protection des renseignements personnels*, qui limite la divulgation de « renseignements concernant leur état physique ou mental ». Voir la *Loi sur la protection des renseignements personnels*, art. 77.

47. En vertu du nouvel art. 11.16, le ministre peut désigner une personne, notamment le directeur du SCRS ou un employé, pour l'application du nouvel art. 11.17. Toutefois, une autorisation prévue au par. 11.17 ne peut être donnée que par une seule personne à la fois.

48. Comme le prévoit le nouveau par. 27.1(6), toute audience tenue à la Cour fédérale relativement à des questions liées à l'art. 27 est entendue à huis clos en conformité avec les règlements d'application de l'art. 28 de la Loi sur le SCRS.

49. *Loi visant à encourager et à faciliter la communication d'information entre les institutions fédérales afin de protéger le Canada contre des activités qui portent atteinte à la sécurité du Canada* (titre abrégé *: Loi sur la communication d'information ayant trait à la sécurité du Canada* [LCISC]), L.C. 2015, ch. 20, art. 2.

50. *Loi antiterroriste de 2015*.

51. LCISC, art. 3.

52. L'annexe 3 de la LCISC énumère les organismes suivants : Agence canadienne d'inspection des aliments; Agence de la santé publique du Canada; Agence des services frontaliers du Canada; Agence du revenu du Canada; Centre d'analyse des opérations et déclarations financières du Canada; Centre de la sécurité des télécommunications; Commission canadienne de sûreté nucléaire; Forces armées canadiennes; Gendarmerie royale du Canada; Ministère de la Citoyenneté et de l'Immigration; Ministère de la Défense nationale; Ministère de la Santé; Ministère de la Sécurité publique et de la Protection civile; Ministère des Affaires étrangères, du Commerce et du Développement; Ministère des Finances; Ministère des Transports; Service canadien du renseignement de sécurité.

53. SECU, *Procès-verbal*, 1re session, 42e législature, 14 juin 2016.

54. SECU (2017), recommandations 22 à 26, p. 43 et 44.

55. Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Procès-verbal*, 1re session, 42e législature, 18 octobre 2016.

56. ETHI, *Assurer la sécurité nationale du Canada tout en protégeant le droit à la vie privée des Canadiens : Examen de la Loi sur la communication d'information ayant trait à la sécurité du Canada (LCISC)*, cinquième rapport, 1re session, 42e législature, mai 2017.

57. Gouvernement du Canada (2016).

58. Hill et Knowlton Stratégies, *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*.

59. *Ibid*.

60. Les professeurs Craig Forcese et Kent Roach ont fait valoir dans un mémoire au Comité ETHI que « les activités de protestation et de défense d'une cause ne devraient pas toutes être soustraites au nouveau régime de communication de renseignements. Si leur portée est suffisamment grande, les activités violentes de protestation ou de défense d'une cause *peuvent* poser problème sur le plan de la sécurité nationale ». Voir Craig Forcese et Kent Roach, *Mémoire au Comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique – Analyse et propositions visant la Loi sur la communication d'information ayant trait à la sécurité du Canada*, 3 novembre 2016, p. 5.

61. Voir SECU (2017); ETHI (2017); et Commissariat à la protection de la vie privée du Canada, *Consultation sur le cadre de sécurité nationale du Canada – Mémoire du Commissariat à la protection de la vie privée du Canada à l'intention de la Direction générale des politiques de la sécurité nationale de Sécurité publique Canada*, 5 décembre 2016.

62. ETHI (2017), recommandation 10, p. 70.

63. ETHI (2017); et Commissariat à la protection de la vie privée du Canada (2016).

64. *Loi de 2002 sur la sécurité publique*, L.C. 2004, ch. 15.

65. *Loi sur l'aéronautique*, L.R.C. 1985, ch. A-2.

66. *Loi sur la sûreté des déplacements aériens*, L.C. 2015, ch. 20, art. 11.

67. Au sens de l'art. 2 et du par. 83.01(1) du *Code criminel*. Il convient de noter que le sous-al. 8(1)b)(i) de la *Loi sur la sûreté des déplacements aériens* vise certaines infractions de terrorisme, par opposition à l'ensemble des infractions de terrorisme inscrites au *Code criminel*.

68. Gouvernement du Canada (2016); et SECU (2017).

69. Cette annexe comporte 34 éléments, dont le nom de la personne, sa date de naissance, sa citoyenneté, son sexe, les noms de l'agence de voyage et de l'agent de voyage ayant effectué les arrangements de voyage de la personne, une indication que le billet de la personne pour le vol est un billet aller simple, la ville ou le pays où le voyage débute, les villes inscrites à l'itinéraire, la destination de la personne, les sièges attribués au préalable, les numéros d'étiquette des bagages de la personne, l'adresse de la personne, l'adresse de l'agence de voyage ayant effectué les arrangements de voyage et le mode de paiement du billet de la personne.

70. *Loi sur l'aéronautique*, « Annexe ».

71. *Loi sur la protection des renseignements personnels*, art. 77.

72. *X (Re)*, par. 50.

73. Le ministre peut prolonger la période de 60 jours s'il existe des circonstances exceptionnelles (voir *Loi sur la sûreté des déplacements aériens*, par. 15(2)).

74. SECU (2017), recommandation 36, p. 45.

75. *Charkaoui c. Canada (Citoyenneté et Immigration)*, 2007 CSC 9.

76. *Loi sur la sûreté des déplacements aériens*, art. 16.

77. L'avocat spécial a pour rôle d'agir au nom de la personne visée dans le cadre de l'instance relative à un certificat de sécurité. Depuis 2008, les avocats spéciaux prennent connaissance de la preuve qui pèse contre la personne nommée au certificat de sécurité, et ont ensuite la possibilité de contester les affirmations du ministre selon lesquelles ces éléments de preuve confidentiels ne peuvent être communiqués à l'intéressé. Ils peuvent aussi contester la pertinence, la fiabilité et la suffisance des éléments de preuve confidentiels ainsi que l'importance qui devrait leur être accordée. Ces renseignements seront ensuite communiqués à l'intéressé sous forme de résumé pour lui permettre d'être raisonnablement informé de la preuve retenue contre lui. Une fois que l'avocat spécial a obtenu les éléments de preuve confidentiels, il ne peut communiquer avec qui que ce soit au sujet de l'instance, y compris avec la personne nommée au certificat de sécurité, sans avoir d'abord obtenu du juge une autorisation en ce sens.

78. SECU (2017), recommandation 33, p. 45.

79. Gouvernement du Canada (2016), p. 15.

80. Hill et Knowlton Stratégies, *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*.

81. *Ibid*.

82. *Ibid*.

83. *Ibid*.

84. *Ibid*.

85. *Ibid*.

86. SECU (2017), recommandations 16 à 21, p. 42 et 43.

87. *Loi antiterroriste*, L.C. 2001, ch. 41. À noter que la liste d'entités prévue au par. 83.05(1) du *Code criminel* ne constitue pas la seule liste applicable; voir Bureau du surintendant des institutions financières, *Lutte contre le financement d'activités terroristes*.

88. *Code criminel*, par. 83.01(1).

89. À l'heure actuelle, le gouvernement du Canada tient des listes d'entités terroristes en vertu de trois règlements : le *Règlement établissant une liste d'entités*, pris en vertu du paragraphe 83.05(1) du *Code criminel*, le *Règlement d'application des résolutions des Nations Unies sur la lutte contre le terrorisme* et le *Règlement d'application des résolutions des Nations Unies sur Al-Qaïda et le Taliban*. Voir Bureau du surintendant des institutions financières, *Lutte contre le financement d'activités terroristes*.

90. Sécurité publique Canada, *Entités terroristes inscrites*.

91. Le simple fait d'être membre d'un groupe terroriste ne constitue pas en soi une infraction criminelle.

92. Sécurité publique Canada, *Entités terroristes inscrites*.

93. *Ibid*.

94. SECU, *Témoignages*, 2e session, 41e législature, 10 mars 2015, 0915 (l'hon. Peter MacKay, ministre de la Justice et procureur général du Canada).

95. SECU (2017), p. 28.

96. *Ibid*.

97. *Demande fondée sur l'art. 83.28 du Code criminel (Re)*, 2004 CSC 42; et *Vancouver Sun (Re)*, 2004 CSC 43.

98. *Loi sur le système de justice pénale pour les adolescents*, L.C. 2002, ch. 1.

99. *Ibid*., sous-al. 3(1)a)(i) et 3(1)d)(i).

100. Laura Barnett *et al.*, *Résumé législatif du projet de loi C-10 : Loi édictant la Loi sur la justice pour les victimes d'actes de terrorisme et modifiant la Loi sur l'immunité des États, le Code criminel, la Loi réglementant certaines drogues et autres substances, la Loi sur le système correctionnel et la mise en liberté sous condition, la Loi sur le système de justice pénale pour les adolescents, la Loi sur l'immigration et la protection des réfugiés et d'autres lois*, publication nº 41-1-C10-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 17 février 2012.

101. *Décret sur les passeports canadiens*, TR/81-86. Voir, par exemple, l'art. 10.1 du *Décret*.