Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Septembre 2025

Canada

Le Comité des parlementaires sur la sécurité nationale et le renseignement
Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement

CP104-7/2025E-PDF
ISBN 978-0-660-77739-9

C.P. 8015, Succursale T, Ottawa, Canada, K1G 5A6
www.nsicop-cpsnr.ca

Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Mme Patricia Lattanzio, députée
Présidente

Présenté au premier ministre le 4 mars 2025
Version révisée présentée au Parlement en septembre 2025

Révisions

En application du paragraphe 21(2) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (Loi sur le CPSNR), le Comité peut présenter un rapport spécial au premier ministre et aux ministres concernés sur toute question liée à son mandat. Conformément au paragraphe 21(5) de la Loi sur le CPSNR, le premier ministre peut, après consultation du président du Comité, ordonner au Comité de lui présenter un rapport révisé qui ne contient pas de renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationale ou aux relations internationales, ou qui sont protégés par le secret professionnel de l'avocat, selon le premier ministre.

Le présent document constitue un rapport révisé du Rapport spécial fourni au premier ministre. À ce moment, le document portait la classification Très secret//Renseignement spécial//Réservé aux Canadiens//Réservé aux organismes d'application de la loi. Des révisions ont été apportées de façon à retirer l'information dont la communication, selon le premier ministre, porterait atteinte à la sécurité ou à la défense nationale ou qui est protégée par le secret professionnel de l'avocat. Lorsque la suppression n'affecte pas la lisibilité du texte, le Comité signale la suppression par trois astérisques (***) dans le texte du présent document. À l'inverse, le Comité révise le document pour résumer l'information retirée. Ces passages sont signalés par trois astérisques au début et à la fin du résumé et sont placés entre crochets (voir l'exemple ci-dessous).

EXEMPLE : [*** Les passages révisés sont signalés par trois astérisques en début et en fin de phrase, et le résumé est placé entre crochets. ***]

Le Comité des parlementaires sur la sécurité nationale et le renseignement

44e législature

Mme Patricia Lattanzio, députée, présidente

M. Stéphane Bergeron, député

M. Don Davies, député

L'honorable Patricia Duncan, sénatrice

M. Darren Fisher, député
(membre jusqu'au 20 décembre 2024)

Mme Iqra Khalid, députée
(membre jusqu'au 17 septembre 2023)

L'honorable Marty Klyne, sénateur

L'honorable Frances Lankin, C.P., C.M., sénatrice
(membre jusqu'au 20 octobre 2024)

M. James Maloney, député
(membre jusqu'au 17 septembre 2023)

L'honorable David J. McGuinty, C.P., député
(président du 6 novembre 2017 au 20 décembre 2024)

M. Rob Morrison, député

M. Alex Ruff, C.S.M., C.D., député

Mme Brenda Shanahan, députée

Table des matières

Mise en contexte

1. En juillet 2023, Statistique Canada a déclaré que 95 % des Canadiens âgés de 15 ans et plus utilisent Internet et qu'un nombre croissant de Canadiens se familiarisent avec les nouvelles technologies et les intègrent à leur routine quotidienne chaque année[1]. Des avancées comme l'utilisation de téléphones intelligents et d'applications de messagerie instantanée ont facilité la communication, devenue instantanée, entre les personnes et ont généré des avantages économiques et sociaux importants.

2. Ces technologies génèrent aussi une quantité considérable de renseignements personnels qui présentent, parfois, un intérêt pour l'État. Précisément, les organismes de sécurité et de renseignement du Canada pourraient devoir accéder à ces renseignements dans le cadre d'enquêtes sur la sécurité nationale. Effectivement, ces technologies sont utilisées dans la planification, la coordination, le financement et la perpétration de menaces envers la sécurité publique et la sécurité nationale du Canada, comme le terrorisme, le crime organisé grave et l'ingérence étrangère.

3. L'interception des communications électroniques, ainsi que la fouille, la perquisition et la saisie des informations électroniques, est une pratique autorisée par les tribunaux et connue sous le nom d'accès légal[2]. Les organismes de sécurité et de renseignement du Canada déclarent faire face depuis un moment à des défis grandissants quant à leur capacité d'utiliser des techniques d'accès légal. Ils indiquent que le chiffrement et la quantité, la variété et la vitesse croissantes des données numériques rendent difficile, voire impossible de recueillir l'information requise pour mener des enquêtes efficaces. De plus, ils affirment que la nature mondiale de l'Internet remet en question la législation rédigée à une époque où l'information et les fournisseurs de services de communication (FSC) résidaient en grande partie à l'intérieur des frontières du Canada.

4. Cependant, les défenseurs de la vie privée, les groupes de la société civile, les universitaires et les experts en cybersécurité et en droit affirment que le gouvernement n'a pas réussi à moderniser l'accès légal pour les organismes de sécurité et de renseignement qui, selon eux, sont également en mesure de tirer parti des capacités d'enquête offertes par les nouvelles technologies[3]. Ils avertissent également que les efforts visant à faciliter l'accès de la police et des services de renseignement aux communications ou aux données chiffrées ou à contourner leur chiffrement affaiblissent fondamentalement la cybersécurité dans son ensemble, érodent la confiance du public et menacent les valeurs démocratiques fondamentales[4].

1 Statistique Canada, « Enquête canadienne sur l'utilisation de l'Internet, 2022 », 7 juillet 2023.
2 Industrie Canada, Ministère de la Justice et Solliciteur général Canada, Accès légal – Document de consultation, 2002.
3 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), novembre 2023.
4 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le CPSNR, novembre 2023; et Siena Anstis, Ronald J. Deibert, Camila Franco et Zoe Panday, « Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the NSICOP », 30 juin 2023.

5. En 2011, deux récits concurrents ont vu le jour. L'un décrivait un « âge d'or de la surveillance », où les progrès technologiques ont permis aux gouvernements d'avoir un accès sans précédent à l'information sur des personnes, ainsi que la capacité de stocker et d'exploiter cette information pour obtenir encore plus de détails que le contenu de la communication ne pouvait révéler par lui-même[5]. L'autre mettait en garde contre le phénomène de la « perte d'accès aux informations », que les praticiens de la sécurité et du renseignement désignaient comme l'écart grandissant entre l'autorisation légale d'accéder aux communications électroniques en vertu d'une autorisation judiciaire et la capacité pratique d'obtenir ces communications[6]. Souvent présenté comme un jeu à somme nulle, le débat oppose, d'un côté, la responsabilité du gouvernement de prévenir les menaces envers la sécurité nationale et d'y répondre et, de l'autre, le droit à la vie privée des Canadiens. Le débat est essentiellement sclérosé depuis ce temps.

6. Le présent examen vise notamment à faire avancer le débat au-delà de cette impasse et à relancer la discussion. Souvent, les organismes de sécurité et de renseignement hésitent à décrire publiquement les vulnérabilités opérationnelles hautement sensibles, comme celles qui, selon eux, sont causées par des défis d'accès légal, afin de ne pas fournir aux adversaires plus d'informations sur la façon de dissimuler leurs activités. Le Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité) a accès à ces informations. Cet accès lui permet d'examiner la mesure dans laquelle les défis d'accès légal nuisent à la capacité des organismes de sécurité et de renseignement de remplir leurs mandats, et d'examiner les efforts du gouvernement pour répondre à ces défis.

Portée et approche

7. Le 18 août 2022, le Comité a annoncé son examen du cadre législatif, réglementaire, stratégique et financier de l'accès légal aux communications par les organismes de sécurité et de renseignement, les défis découlant des technologies nouvelles et émergentes, et les limites du cadre actuel, énoncé dans le cadre de référence figurant à l'annexe A[7]. Les objectifs de cet examen consistent à examiner :

- l'état actuel de l'accès légal, y compris les défis cernés par l'appareil de la sécurité nationale et du renseignement;
- les préoccupations et les critiques soulevées par des experts de la société civile et de la protection de la vie privée au sujet de la modernisation des pouvoirs dans ce domaine;
- les défis technologiques liés à l'accès légal, y compris l'interception légale des communications et la recherche et la saisie de données liées aux communications;
- la mesure dans laquelle l'appareil de la sécurité et du renseignement a atténué les défis de la perte d'accès aux informations au moyen de la technologie, de politiques et de la coopération avec les FSC;
- la mesure dans laquelle des lacunes subsistent pour faire face à l'incidence des technologies nouvelles et émergentes sur l'accès légal aux communications.

5 Peter Swire et Kenesa Ahmad, « Encryption and Globalization », *Ohio State Public Law Working Paper No. 157, Columbia Science and Technology Law Review, Vol. 23, 2012*, 17 novembre 2011.

6 Avocate générale du Federal Bureau of Investigation Valerie Caproni, « Statement before the United States House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security », Washington D.C., 17 février 2011.

7 CPSNR, « Le Comité des parlementaires sur la sécurité nationale et le renseignement lance un examen de l'interception légale des communications dans le cadre d'activités de sécurité et de renseignement », communiqué de presse, 18 août 2022.

8. L'examen a porté sur les informations du 1er janvier 2012 au 9 janvier 2025 et comprenait les organisations suivantes :

- Centre de la sécurité des télécommunications (CST);
- Gendarmerie royale du Canada (GRC);
- ministère de la Justice;
- ministère de la Sécurité publique et de la Protection civile (Sécurité publique Canada);
- Service canadien du renseignement de sécurité (SCRS).

9. Pour appuyer son examen, le Comité a demandé des documents au SCRS, au CST, au ministère de la Justice, à la GRC et à Sécurité publique Canada, et s'est appuyé sur les exposés du Secrétariat et sur les réponses des ministères à des questions écrites. De hauts fonctionnaires du SCRS, du CST, de la GRC, de SP et du ministère de la Justice ont comparu devant le Comité, parfois à plus d'une reprise. Au cours de la dernière phase de son examen, le Comité a rencontré le ministre de la Justice et le ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales. Le Comité a également sollicité les commentaires d'intervenants de l'extérieur du gouvernement fédéral, y compris de représentants des FSC, de la société civile et de la communauté juridique. Le Comité remercie les ministres, les fonctionnaires et tous les présentateurs de leur temps et de leur expertise. La liste complète des témoins et des participants figure à l'annexe B.

10. Afin de mieux comprendre les préoccupations relatives à l'accès légal, le Comité a commandé ou demandé des documents de recherche à des experts en protection de la vie privée, en droit et en cybersécurité, à la suite d'un appel de documents. Il tient à remercier le professeur Benjamin J. Goold, le professeur Vivek Krishnamurthy, le professeur Michael Geist et le professeur Ron Deibert du Citizen Lab pour leurs contributions[8].

11. En examinant les documents présentés dans le cadre de cet examen, le Comité a décidé de répondre aux questions suivantes :

- Les défis d'accès légal du Canada sont-ils aussi préoccupants pour les enquêtes sur la sécurité nationale que le prétendent les organismes de sécurité et de renseignement?
- Le gouvernement a-t-il réussi à trouver des solutions à ces défis ou à les atténuer?
- De quelle manière le gouvernement du Canada facilite-t-il ou permet-il la tenue d'enquêtes sur la sécurité nationale tout en protégeant le droit des Canadiens à la vie privée?

12. Le présent examen traite en dernière analyse de l'exercice des pouvoirs de l'État. Le mandat du Comité réduit sa portée aux activités de sécurité nationale du gouvernement fédéral[9]. Bien que le Comité reconnaisse que des entités commerciales du Canada et de l'étranger recueillent des renseignements personnels en ligne sur des Canadiens et que ces pratiques soulèvent d'importantes questions sur le plan de la vie privée pour les législateurs, ces enjeux dépassent la portée du présent examen.

---

8 Le Comité accuse réception des documents suivants : Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance*, novembre 2023; Siena Anstis, Ronald J. Deibert, Camila Franco et Zoe Panday, « Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the NSICOP », 30 juin 2023; Michael Geist, *Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes Internet*, document commandé par le CPSNR, mai 2024; et Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, 30 août 2023.

9 Loi sur le CPSNR (L.C. 2017, ch. 15), articles 8 et 13.

Chapitre 1 : La vie privée et la sécurité dans le monde numérique

13. Le droit individuel à la vie privée est fondamental pour la société canadienne[10]. Il garantit que les gens peuvent mener leur vie sans être soumis au contrôle d'autrui, en particulier du gouvernement. Par conséquent, le gouvernement a l'obligation de protéger ce droit tout en s'acquittant de sa responsabilité d'assurer la sécurité publique et de protéger la sécurité nationale[11]. Ce point est crucial, car l'accès légal représente l'un des pouvoirs les plus intrusifs de l'État. Nonobstant la capacité grandissante des entités commerciales de recueillir des renseignements personnels, seul l'État est habilité à porter atteinte à la liberté personnelle d'un individu, y compris par l'arrestation, la détention, la poursuite et l'emprisonnement. Le présent chapitre vise à fournir une compréhension de base du concept de la vie privée dans le contexte de l'accès légal et de l'intersection de la vie privée et de la sécurité.

Comprendre le droit à la vie privée

14. Le droit à la vie privée est un concept à multiples facettes qui repose sur plusieurs principes clés[12]. Dans le contexte du présent examen, il est surtout question de l'aspect informationnel de la vie privée : le droit d'une personne de protéger ses informations et d'exercer un contrôle sur la manière dont ces informations sont utilisées par l'État. Il se rapporte également aux attentes en matière d'anonymat et de confidentialité, en mettant l'accent sur la protection de la capacité d'une personne à garder ses renseignements personnels à l'abri du regard du public[13].

15. Le droit à la vie privée est aussi hautement contextuel. Le Conseil des académies canadiennes a constaté que les opinions et les décisions des personnes concernant la protection de la vie privée changent en fonction de divers facteurs, y compris leurs circonstances sociales, géographiques, historiques et culturelles[14].

10 Commissariat à la protection de la vie privée du Canada (CPVP), *Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur l'étude des outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada*, août 2022.

11 Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale, 2016*, 2016; et Industrie Canada, Ministère de la Justice et Solliciteur général Canada, Accès légal – Document de consultation, 2002.

12 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, juin 2015.

13 *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212.

14 Conseil des académies canadiennes, *Connexions vulnérables : Le comité d'experts sur la sécurité publique à l'ère du numérique*, mars 2023.

16. Alors que le droit à la vie privée est souvent défini dans le contexte des droits individuels, le droit à la vie privée a également une dimension collective :

> Également, le droit à la vie privée est important parce qu'il constitue le fondement de l'exercice d'autres libertés et droits fondamentaux, au premier rang desquels figurent la liberté d'expression et la liberté d'association. En permettant aux individus de limiter l'accès à leurs communications – et d'établir à qui ils transmettent leurs idées et leurs renseignements –, le droit à la vie privée favorise la création d'espaces dans lesquels les opinions et croyances différentes peuvent s'épanouir[15].

17. Selon la British Columbia Civil Liberties Association (BCCLA), une association de la Colombie-Britannique sur les libertés civiles, la vie privée [traduction] « est un besoin psychologique et un droit fondamental sur lequel reposent bon nombre d'autres droits essentiels. […] Le droit à la vie privée sert donc de fondement aux libertés fondamentales protégées par l'article 2 de la *Charte des droits et libertés* : la liberté de conscience, de religion, d'expression, de pensée, de croyance et d'opinion qui repose au cœur même des démocraties libérales comme le Canada, ainsi qu'aux droits à la liberté reconnus à l'article 7 [de la *Charte canadienne des droits et libertés* (la Charte)][16]. »

18. La Cour suprême du Canada a décrit la vie privée comme une « considération fondamentale d'une société libre », affirmant :

> Bien que la vie privée d'une personne soit d'une importance primordiale pour celle-ci, la protection de la vie privée est également dans l'intérêt de la société dans son ensemble. La vie privée ne saurait donc être rejetée en tant que simple préoccupation personnelle : il y a chevauchement entre certaines préoccupations personnelles relatives à la vie privée et les intérêts du public[17].

La position de la Cour suprême reflète une approche normative en matière de protection de la vie privée. Cette approche porte [traduction] « non seulement sur ce qu'est la vie privée, mais aussi sur ce qu'elle devrait être », en utilisant une « perspective plus large de la façon dont nous voulons vivre en tant que société[18] ».

19. Il est de plus en plus difficile de définir à quoi les normes entourant le droit à la vie privée devraient ressembler. Les recherches laissent entendre que les conceptions et les attentes en matière de droit à la vie privée évoluent à mesure que la technologie numérique[19] transforme la vie quotidienne des Canadiens[20]. Bien que le degré d'adoption et d'utilisation puisse varier d'une personne à une autre, le Conseil des académies canadiennes fait valoir que l'omniprésence des technologies numériques est telle que tout le monde au Canada peut être considéré comme « numérique par défaut »[21]. Étant donné la quantité croissante

15 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le CPSNR, novembre 2023.
16 British Columbia Civil Liberties Association (BCCLA), comparution devant le CPSNR, 1er octobre 2024.
17 *Sherman (Succession) c. Donovan*, 2021 CSC 25, [2021] 2 R.C.S. 75.
18 Ann Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy Makers*, août 2011.
19 La technologie numérique renvoie à *l'utilisation de systèmes, d'outils et de dispositifs numériques* qui traitent, stockent et transmettent des données sous forme électronique, par opposition aux technologies analogiques qui l'ont précédée.
20 Conseil des académies canadiennes, *Connexions vulnérables : Le comité d'experts sur la sécurité publique à l'ère du numérique*, mars 2023.
21 Conseil des académies canadiennes, *Connexions vulnérables : Le comité d'experts sur la sécurité publique à l'ère du numérique*, mars 2023.

de renseignements personnels recueillis par une foule d'entités, chacune ayant sa propre approche pour protéger ces données[22], les considérations relatives à la protection de la vie privée ne sont plus centrées sur le maintien du secret de l'information. Elles se sont plutôt étendues pour inclure [traduction] « la régulation du flux d'informations vers certains, la restriction des informations pour certains et l'ouverture à d'autres[23] ».

Équilibre entre la vie privée et la sécurité

20. Les organismes d'application de la loi et de sécurité sont chargés de protéger la sécurité nationale et la sécurité publique[24]. Pour y parvenir efficacement, ils peuvent devoir accéder à des communications privées. Les techniques de collecte et de surveillance peuvent générer des pistes, révéler des menaces et aider à trouver des personnes ou des groupes impliqués dans des menaces comme le terrorisme, le crime organisé grave, l'espionnage et l'ingérence étrangère et à enquêter sur ceux-ci[25]. Cet accès entrave nécessairement le droit à la vie privée d'une personne[26].

21. La collecte de renseignements personnels par l'État diffère d'une telle collecte par des entités commerciales en raison des pouvoirs coercitifs de l'État et de l'aspect souvent subreptice de la surveillance électronique menée par les organismes de sécurité nationale et de renseignement[27]. Outre les droits liés à la vie privée auxquels touchent directement les activités d'accès légal, comme la surveillance électronique, l'accès légal peut aussi conduire à d'autres activités intrusives ou coercitives de l'État, comme la fouille, la saisie et la perquisition de biens et la communication d'informations à d'autres États. Dans la plupart des démocraties aux vues similaires, de telles infractions doivent être prévues par la loi, poursuivre un but légitime et être nécessaires et proportionnées[28]. (Le cadre juridique du Canada régissant l'accès légal sera décrit dans le chapitre suivant.)

22. La question de savoir si une telle intrusion est appropriée, notamment dans quelle mesure, fait l'objet d'un débat acharné, réduisant souvent la tension entre la vie privée et la sécurité à un jeu à somme nulle. Certains soutiennent que de tels pouvoirs ne devraient pas exister du tout; d'autres acceptent les pouvoirs, mais insistent sur la nécessité d'encadrer leur utilisation au moyen de mesures de protection rigoureuses[29]. D'autres contestent également l'idée que l'autorisation judiciaire d'accès légal suffit pour répondre aux préoccupations en matière de protection de la vie privée. M. Goold souligne que :

> [b]ien qu'elle soit importante, la responsabilité légale par le biais de la surveillance judiciaire ne permet qu'en partie de voir à ce que la police soit assujettie convenablement à la primauté du droit. En outre, il doit y avoir une transparence de l'éventail des pouvoirs et des techniques d'enquête dont elle dispose[30].

22 Michael Geist, *Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes Internet*, document commandé par le CPSNR, mai 2024.
23 Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age*, 2018.
24 Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale, 2016*, 2016.
25 Industrie Canada, Ministère de la Justice et Solliciteur général Canada, *Accès légal – Document de consultation*, 2002.
26 Industrie Canada, Ministère de la Justice et Solliciteur général Canada, *Accès légal – Document de consultation*, 2002.
27 BCCLA, comparution devant le CPSNR, 1er octobre 2024.
28 Commissaire aux droits de l'homme du Conseil de l'Europe, *Des logiciels espions très intrusifs menacent l'essence des droits humains*, janvier 2023.
29 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, juin 2015.
30 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le CPSNR, novembre 2023.

Toutes les parties ont demandé de nuancer davantage le débat, affirmant que la protection de la vie privée et la sécurité font partie intégrante de la démocratie canadienne et qu'il existe des moyens de respecter ces deux aspects simultanément[31].

23. Selon la BCCLA, l'autorisation judiciaire de l'accès légal est cruciale, quoiqu'insuffisante, particulièrement pour ce qui est des enquêtes du Service canadien du renseignement de sécurité (SCRS) où [traduction] « il demeure possible que le SCRS ne fasse pas suffisamment preuve de franchise devant la Cour pour assurer pleinement la protection des droits » lorsqu'il présente une demande de mandat[32]. Cette préoccupation découle d'un jugement marquant de la Cour fédérale de 2016 selon lequel le SCRS avait manqué à son obligation de franchise dans le cadre de nombreuses demandes de mandats[33]. Dans une décision subséquente, la Cour fédérale a fait remarquer que les manquements répétés donnaient à penser « qu'à l'échelle organisationnelle, dans une certaine mesure, les différents intervenants ont fait peu de cas de l'obligation de franchise et – malheureusement – de la primauté du droit ou, tout au moins, ont adopté à leur égard une attitude cavalière[34]. » Le SCRS souligne qu'il a depuis adapté ses pratiques avec la Cour fédérale afin de mieux satisfaire à son obligation de franchise et qu'il croit que la confiance de la Cour fédérale a été restaurée[35].

24. Le commissaire à la protection de la vie privée a déclaré que la transparence quant à la façon dont les organismes de sécurité et de renseignement considèrent les préoccupations en matière de protection de la vie privée peut agir comme un « moyen pour accentuer » la confiance envers les institutions gouvernementales[36]. Autrement dit, si ces organismes mettent en place des mécanismes et des pratiques pour démontrer comment ils mettent la protection de la vie privée au premier plan de leurs délibérations et de leurs actions, le public est plus susceptible de faire confiance à la nécessité des pouvoirs et outils d'enquête proposés. Cela favorise le consentement du public et la légitimité lorsqu'il s'agit d'actions qui pourraient nuire aux droits des Canadiens garantis par la Charte.

25. Par conséquent, certains défenseurs de la vie privée ont demandé une plus grande transparence des organismes d'application de la loi et de sécurité dans l'exécution des activités d'accès légal[37]. Les mécanismes de transparence comprennent des rapports réguliers sur les demandes et l'accès du gouvernement aux renseignements personnels, une plus grande participation des organisations de protection de la vie privée dans la création de capacités d'accès légal et l'obligation légale d'effectuer des évaluations des facteurs relatifs à la vie privée (EFVP)[38].

31 CPVP, comparution devant le CPSNR, 18 juin 2024.
32 BCCLA, comparution devant le CPSNR, 1er octobre 2024.
33 2016 CF [Cour fédérale] 1105, version publique.
34 2020 CF 616, version publique.
35 SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.
36 CPVP, *Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur l'étude des outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada*, août 2022.
37 CPVP, comparution devant le CPSNR, 18 juin 2024.
38 CPVP, comparution devant le CPSNR, 18 juin 2024.

26. M. Goold met en garde contre le fait d'établir ainsi un lien entre la confiance et la transparence :

> [La] promotion de la confiance sert de motif justifiant une transparence accrue [et] peut sembler ne poser aucun problème, mais l'hypothèse selon laquelle une plus grande transparence est toujours et inévitablement une bonne chose mérite d'être examinée de plus près. C'est particulièrement le cas lorsqu'il s'agit de l'utilisation de technologies de surveillance par la police et les services de sécurité. Bien que la transparence soit souvent citée comme une condition préalable nécessaire à la responsabilité institutionnelle, elle peut également jouer un rôle dans la normalisation des activités qui devraient être considérées comme exceptionnelles[39].

27. De même, M. Goold demande un changement dans la façon dont le gouvernement entame une réforme législative visant à répondre aux difficultés liées à l'accès légal afin que les Canadiens préoccupés par la protection de la vie privée ne sentent pas qu'ils doivent « être sur la défensive »[40]. Il affirme que le gouvernement doit mieux justifier la nécessité d'élargir les pouvoirs et les outils de surveillance de manière plus transparente[41]. Ceci est particulièrement important, car une fois que le droit à la vie privée est cédé en raison de nouvelles autorisations ou de l'adoption d'une nouvelle technologie, il est rare de faire marche arrière :

> Une fois accordés, les pouvoirs conférés aux agents de l'État comme la police sont rarement retirés ou réduits. De même, avant d'étendre les capacités de surveillance de l'État pour permettre à la police et aux services de sécurité d'utiliser des outils d'enquête sur appareil ou d'autres formes de piratage légal, les législateurs et le public doivent prendre en compte le risque que ces capacités soient utilisées à mauvais escient à l'avenir[42].

28. Le Comité compte se pencher sur ces risques et ceux soulevés par l'appareil de la sécurité et du renseignement dans le présent rapport.

39 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le CPSNR, novembre 2023.
40 Benjamin J. Goold, exposé devant le CPSNR, 21 mai 2024.
41 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le CPSNR, novembre 2023.
42 Benjamin J. Goold, *Accès légal, droit à la vie privée et confiance – Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement*, document commandé par le CPSNR, novembre 2023.

Chapitre 2 : Le cadre juridique de l'accès légal au Canada

29. L'accès légal fait référence à l'interception des communications électroniques, ainsi qu'à la fouille et à la saisie d'informations électroniques, autorisées par les tribunaux, conformément au cadre juridique du Canada[43]. Le présent chapitre décrit certains des droits et libertés garantis par la *Charte canadienne des droits et libertés* (la Charte), ainsi que les pouvoirs prévus dans le *Code criminel*, la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS), la *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) et toute autre loi pertinente, ainsi que la position du Canada par rapport à ses partenaires de l'étranger aux vues similaires dans la réponse aux défis de l'accès légal. La jurisprudence a également joué un rôle important dans les modalités d'utilisation des techniques et des outils d'accès légal par les organismes d'application de la loi et de sécurité. Le présent chapitre décrit de quelle manière les décisions de la Cour suprême en 2014 (*R. c. Spencer*) et en 2024 (*R. c. Bykovets*) ont façonné l'accès légal.

La *Charte canadienne des droits et libertés*

30. La Charte[44] entérine et protège les droits individuels des Canadiens contre une ingérence indue par le gouvernement[45]. Inscrite dans la Constitution, la Charte fait autorité : toutes les lois du Canada doivent être conformes aux règles ou principes qu'elle énonce[46]. Dans le contexte de l'accès légal, un droit conféré par la Charte est particulièrement important, à savoir l'article 8, qui stipule que « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. » L'article 8 est considéré comme une protection de l'attente raisonnable en matière de vie privée[47]. Les activités des organismes d'application de la loi et de sécurité doivent se conformer à l'article 8, sinon elles peuvent être contestées devant les tribunaux[48]. L'article 8 stipule qu'une atteinte à l'attente raisonnable d'une personne en matière de vie privée exige une certaine forme d'autorisation légale, qui correspond généralement à l'autorisation judiciaire préalable[49].

31. L'article 8 de la Charte protège les Canadiens et les personnes au Canada contre les fouilles et les perquisitions *abusives* par des enquêteurs du gouvernement. Peu après l'entrée en vigueur de la Charte, la Cour suprême a statué que l'article 8 visait à prévenir les fouilles et les perquisitions abusives, rendant présomptivement abusive toute fouille ou perquisition réalisée sans mandat[50]. Quelques années plus tard, la Cour suprême a statué qu'une

43 Industrie Canada, ministère de la Justice et Solliciteur général Canada, *Accès légal – Document de consultation*, 2002.
44 *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*, ch. 11 (R.-U.).
45 Henri Brun, Guy Tremblay et Eugénie Brouillet, *Droit constitutionnel,* 5e édition, 2008.
46 Henri Brun, Guy Tremblay et Eugénie Brouillet, *Droit constitutionnel,* 5e édition, 2008.
47 Steve Penney, *The Digitization of Section 8 of the Charter: Reform or Revolution?*, Supreme Court Law Review, 2014.
48 Henri Brun, Guy Tremblay et Eugénie Brouillet, *Droit constitutionnel,* 5e édition, 2008.
49 Henri Brun, Guy Tremblay et Eugénie Brouillet, *Droit constitutionnel,* 5e édition, 2008.
50 *Hunter c. Southam*, [1984] 2 RCS 145.

fouille ou une perquisition non autorisée par la loi était abusive[51]. Conformément aux dispositions autorisant la surveillance électronique, les enquêteurs du gouvernement doivent habituellement obtenir une autorisation judiciaire avant d'effectuer une fouille; c'est le cas pour les pouvoirs conférés par les mandats prévus dans le *Code criminel* et la Loi sur le SCRS[52]. Le seuil requis pour obtenir l'autorisation dépend généralement du niveau d'atteinte à l'attente raisonnable d'une personne en matière de vie privée, et un seuil plus élevé sera requis pour les atteintes plus graves.

32. La fouille est une technique d'enquête qui porte atteinte à l'attente raisonnable d'une personne en matière de vie privée[53]. Si une technique d'enquête ne porte pas atteinte à cette attente, il ne s'agit donc pas d'une fouille[54]. Une fouille est considérée comme légale lorsqu'elle n'est pas abusive au titre de l'article 8 de la Charte[55]. Selon la Cour suprême, « [u]ne fouille ne sera pas abusive si elle est autorisée par la loi, si la loi elle-même n'a rien d'abusif et si la fouille n'a pas été effectuée d'une manière abusive[56]. »

Le *Code criminel*

33. La Gendarmerie royale du Canada (GRC) enquête sur les infractions au Canada et à l'étranger liées à la sécurité nationale, au crime organisé transnational et grave, à la criminalité financière et à la cybercriminalité[57]. La GRC s'appuie sur les dispositions du *Code criminel* pour autoriser ses activités d'accès légal. Tous les organismes d'application de la loi au Canada peuvent obtenir une autorisation judiciaire pour l'interception de communications privées, communément appelée écoute électronique, en déposant une demande en vertu de la partie VI du *Code criminel* par l'entremise d'un avocat de la Couronne[58]. Un juge peut autoriser les services de police à intercepter des communications privées sans le consentement ou la connaissance des parties à la communication, à condition que la demande satisfasse aux critères et respecte les mesures de protection énoncées dans l'autorisation[59].

34. Il convient de noter que la partie VI du *Code criminel* s'applique aux interceptions de communications prospectives en temps réel, plutôt qu'aux recherches rétrospectives de communications stockées. Comme l'a décrit le professeur Krishnamurthy,

> Elle est révélatrice de l'ancienne réalité technologique, où les méthodes étaient très différentes selon que l'on cherchât à intercepter des communications en temps réel (p. ex., écoute électronique) ou bien des communications passées (p. ex., perquisition chez un suspect pour y trouver des lettres incriminantes). La partie VI

51 *R. c. Collins*, [1987] 1 RCS 265.
52 Selon le SCRS, la Cour fédérale a déterminé que l'art. 12 de la Loi sur le SCRS confère une autorisation suffisante pour les fouilles qui entravent très peu sur les intérêts en matière de vie privée. SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.
53 Steve Coughlan, *Criminal Procedure*, 3e édition.
54 Steve Coughlan, *Criminal Procedure*, 3e édition.
55 Steve Coughlan, *Criminal Procedure*, 3e édition.
56 *R. c. Collins*, [1987] 1 RCS 265.
57 L'article 18 de la *Loi sur la Gendarmerie royale du Canada* et la common law autorisent la GRC à prévenir les crimes et à mener des enquêtes sur ces derniers, alors que le paragraphe 6(1) de la *Loi sur les infractions en matière de sécurité* fait de la GRC le service de police principal pour les activités criminelles qui constituent une menace pour la sécurité nationale au sens de l'article 2 de la Loi sur le SCRS.
58 *Code criminel*, L.R.C. (1985), ch. C-46, partie VI (Atteintes à la vie privée).
59 La partie VI prévoit d'autres demandes d'écoute électronique, comme les demandes de consentement d'une seule partie.

soumet l'interception de communications en temps réel à des mesures de protection rigoureuses, comme si c'était la pire invasion de la vie privée imaginable de la part d'un État exerçant son pouvoir de faire respecter le droit criminel[60].

35. Compte tenu du seuil élevé imposé pour demander une écoute électronique, les organismes d'application de la loi demanderont d'abord généralement d'autres ordonnances pour recueillir les informations et les éléments de preuve dont ils ont besoin pour atteindre ce seuil. Par exemple, ils peuvent d'abord demander un mandat pour enregistreur de données de transmission qui permet la collecte de renseignements sur les communications (c'est-à-dire les données de transmission, parfois appelées officieusement les métadonnées), mais pas le contenu d'une communication en soi[61].

36. En outre, la complexité de certains outils et techniques d'enquête peut obliger les organismes d'application de la loi à obtenir de multiples autorisations visant plusieurs dispositions du *Code criminel* pour les déployer. Par exemple, le déploiement d'un outil d'enquête sur appareil pourrait nécessiter plusieurs autorisations différentes, y compris une autorisation d'écoute électronique, un mandat pour enregistreur de données de transmission et un mandat général[62]. Les progrès dans les technologies de communication peuvent également amener les organismes d'application de la loi à demander des autorisations judiciaires supplémentaires en vertu du *Code criminel* pour déployer l'outil ou la technique d'enquête en question. Cela peut comprendre une ordonnance d'assistance pour obliger une personne ou une entreprise à aider les organismes d'application de la loi à exécuter une autorisation ou un mandat[63], ou une ordonnance de conservation pour obliger une personne ou une entreprise à conserver des éléments de preuve électroniques jusqu'à l'obtention d'un mandat approprié[64].

La *Loi sur le Service canadien du renseignement de sécurité*

37. En vertu de l'article 12 de la Loi sur le SCRS, le SCRS est chargé de recueillir, au moyen d'enquêtes, l'information sur les activités soupçonnées de constituer des menaces envers la sécurité du Canada et de l'analyser[65]. Ces activités sont définies dans la Loi comme étant l'espionnage ou le sabotage, les activités influencées par l'étranger, le terrorisme et la subversion[66]. Le SCRS est également autorisé à prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères à la collecte d'information et de renseignements sur des États ou des acteurs étrangers au Canada en vertu de l'article 16 de la Loi sur le SCRS.

60 Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, document commandé par le CPSNR, décembre 2023.
61 *Code criminel*, L.R.C. (1985), ch. C-46, art. 492.2.
62 GRC, « Outils d'enquête embarqués (OEE) – Description technique : Ébauche du Projet », août 2022.
63 *Code criminel*, L.R.C. (1985), ch. C-46, art. 487.02.
64 *Code criminel*, L.R.C. (1985), ch. C-46, art. 487.012 et 487.013.
65 Loi sur le SCRS, L.R.C. (1985), ch. C-23, art. 12.
66 Loi sur le SCRS, L.R.C. (1985), ch. C-23, art. 2.

38. Pour appuyer ses mandats de collecte de renseignements, le SCRS peut demander à la Cour fédérale, en vertu de l'article 21 de sa Loi, des mandats[67] pour mener de la surveillance électronique, connus de façon informelle sous le nom de mandats visés par l'article 12 ou l'article 16, selon que ses activités sont visées par son mandat en vertu de l'article 12 ou de l'article 16. En juin 2024, la *Loi concernant la lutte contre l'ingérence étrangère* a modifié la Loi sur le SCRS pour y inclure de nouvelles autorisations liées à l'accès légal[68]. Il s'agit notamment d'un mandat permettant précisément d'obtenir des informations, des dossiers et des documents, et de la possibilité pour le SCRS de présenter des ordonnances de communication. Avant ces modifications, le SCRS ne disposait que d'une seule autorisation conférée par mandat au titre de la Loi pour autoriser les activités portant atteinte à la vie privée, quelles que fussent les répercussions réelles de l'outil ou de la technique d'enquête sur l'attente raisonnable d'une personne en matière de vie privée.

39. Pour obtenir un mandat, le SCRS fournit à la Cour fédérale un affidavit qui décrit suffisamment « la nature et le contexte de la menace en cause, l'état d'avancement de l'enquête, de même que les raisons justifiant l'obtention de pouvoirs d'enquête plus étendus[69]. » Le SCRS doit également démontrer au juge que les critères énoncés dans la Loi sur le SCRS pour délivrer le mandat sont respectés. Contrairement aux mandats demandés en vertu du *Code criminel*, les demandes de mandat du SCRS ne font généralement pas l'objet d'un examen public et de contestations judiciaires par les parties intéressées au même degré, étant donné que les personnes qui font l'objet d'une interception en vertu du mandat n'en sont pas informées. En effet, c'est principalement parce que l'objectif du SCRS est de recueillir des renseignements et non des éléments de preuve susceptibles d'être utilisés dans le cadre d'une poursuite. Cette approche tient aussi compte de la nature sensible de l'information comprise dans les demandes de mandat et des enquêtes sous-jacentes[70]. Pour cette raison, une série de mesures de protection administratives et exécutives, comme l'approbation du ministre, sont requises pour chaque demande[71].

67 La Cour fédérale a déterminé que les art. 12 et 16 de la Loi sur le SCRS confèrent une autorisation légale raisonnable pour les fouilles qui entravent très peu sur les intérêts en matière de vie privée. SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.

68 *Loi concernant la lutte contre l'ingérence étrangère*, L.C. 2024, ch. 16 (sanctionnée le 20 juin 2024).

69 Murray Segal, *Examen du processus de demande de mandats au SCRS*, décembre 2016.

70 Craig Forcese et Leah West, *National Security Law*, 2020; et SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.

71 Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), *Examen de l'OSSNR découlant de la décision 2020 CF 616 de la Cour fédérale*, 2022.

La *Loi sur le Centre de la sécurité des télécommunications*

40. Le CST est l'organisme canadien chargé du renseignement électromagnétique étranger. En vertu de la Loi sur le CST, le CST est chargé de recueillir l'« information ou [les] renseignements sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger, dans la mesure où ces moyens, ces intentions, ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité[72] ». Il est interdit au CST de diriger ses activités de renseignement étranger contre des Canadiens et il doit mettre en place des mesures appropriées pour protéger la vie privée des Canadiens lorsqu'il obtient incidemment de l'information les concernant[73]. Le CST ne dispose d'aucun pouvoir qui lui soit propre en matière d'accès légal au pays[74].

41. L'article 20 de la Loi sur le CST confère au CST le mandat d'assister les organismes fédéraux chargés de l'application de la loi et de la sécurité[75]. Par conséquent, lorsque la GRC et le SCRS obtiennent l'autorisation appropriée pour mener des activités d'accès légal, ils peuvent demander au CST d'aider à la tenue d'opérations, notamment en concevant des moyens techniques ou en interceptant des communications[76]. Lorsqu'il fournit une assistance technique et opérationnelle, le CST est lié par toutes les restrictions et conditions imposées à la GRC ou au SCRS dans l'exécution de l'activité[77].

Autres lois pertinentes

42. Certaines dispositions de la *Loi sur la preuve au Canada* et de la législation sur la protection de la vie privée du Canada, qui comprend la *Loi sur la protection des renseignements personnels*, sont également pertinentes dans l'examen du cadre juridique du Canada en matière d'accès légal.

43. ***Loi sur la preuve au Canada :*** Les articles 37 et 38 de la *Loi sur la preuve au Canada* établissent un régime permettant au gouvernement de s'opposer à la divulgation de renseignements sensibles ou préjudiciables dans le cadre de poursuites judiciaires. En vertu de l'article 37, le gouvernement peut chercher à empêcher la divulgation de renseignements relatifs à un outil ou à une technique d'enquête sensible des organismes d'application de la loi, y compris les techniques d'accès légal. L'article 38 permet au gouvernement de refuser l'accès à des renseignements qui sont sensibles ou préjudiciables aux relations internationales, à la défense nationale ou à la sécurité nationale du Canada, et peut aussi s'appliquer aux outils et aux techniques mis au point et utilisés par les organismes de sécurité et de renseignement. Lorsqu'un organisme invoque un privilège, le tribunal compétent détermine si l'intérêt public visant la prévention du préjudice (c'est-à-dire le maintien du secret) l'emporte sur les intérêts de la partie qui demande la divulgation[78]. Les tribunaux, lors de poursuites criminelles, peuvent ordonner la divulgation lorsqu'ils

72 Loi sur le CST, L.C. 2019, ch. 13, art. 2.
73 Loi sur le CST, L.C. 2019, ch. 13, art. 24.
74 Craig Forcese et Leah West, *National Security Law*, 2020.
75 Loi sur le CST, L.C. 2019, ch. 13, art. 20.
76 Loi sur le CST, L.C. 2019, ch. 13, art. 20; et CST, *Assistance aux partenaires fédéraux*, avril 2021.
77 CST, *Assistance aux partenaires fédéraux*, avril 2021.
78 Loi sur la preuve au Canada, L.R.C. (1985), ch. C-5; et Craig Forcese et Leah West, *National Security Law*, 2020.

déterminent que la balance penche en faveur de l'accusé. La Couronne devra ensuite décider de divulguer les renseignements à la défense, de s'abstenir d'utiliser les renseignements ou de surseoir aux accusations.

44. ***Législation en matière de vie privée :*** La *Loi sur la protection des renseignements personnels* établit la règle de droit en ce qui concerne les pratiques entourant le traitement des renseignements personnels par les ministères et organismes fédéraux, y compris la façon dont ils peuvent être recueillis, utilisés ou communiqués[79]. La *Loi sur la protection des renseignements personnels et les documents électroniques* régit la collecte, l'utilisation et la communication de renseignements personnels par les organisations du secteur privé au Canada[80].

Jurisprudence notable

45. La jurisprudence joue un rôle important dans l'établissement des limites du cadre juridique du Canada. Plus particulièrement, plusieurs décisions clés de la Cour suprême ont façonné la compréhension de ce qui constitue une attente raisonnable en matière de vie privée. La jurisprudence est telle que les organismes d'application de la loi et de renseignement sont généralement tenus d'obtenir une autorisation judiciaire préalable pour recueillir un large éventail de renseignements liés aux communications dans le contexte des activités d'enquête et de collecte d'information.

46. ***Attente raisonnable en matière de vie privée :*** Au cours de la dernière décennie, la Cour suprême a considérablement élargi le champ d'application de ce qui donne lieu à une attente raisonnable en matière de vie privée à l'ère numérique. Dans l'arrêt *R. c. Spencer* (2014), la Cour suprême a conclu à l'unanimité que le lien entre l'identité d'utilisateurs d'Internet et leur utilisation d'Internet suscite des intérêts en matière de vie privée et que les utilisateurs d'Internet ont une attente raisonnable en matière de vie privée. Plus précisément, la Cour a déclaré que les renseignements de base sur les abonnés (RBA) fondés sur une adresse de protocole Internet (IP) connue ont fourni des renseignements sur la vie personnelle d'utilisateurs d'Internet alors qu'il serait raisonnable pour eux de s'attendre à ce qu'ils soient privés[81]. À ce titre, la Cour a déterminé qu'une demande de RBA équivaut à une fouille et nécessite donc une autorisation judiciaire préalable.

47. Plus récemment, dans une décision partagée (5 contre 4) dans l'affaire *R. c. Bykovets* (2024), les juges de la Cour suprême ont déterminé que l'adresse IP d'une personne suscite également une attente raisonnable en matière de vie privée, et qu'une demande à une entreprise privée, comme un fournisseur de services de communication (FSC), pour obtenir cet identificateur équivaut à une fouille. Par conséquent, les organismes d'application de la loi ont besoin d'une autorisation judiciaire préalable pour obtenir ces renseignements[82].

48. ***Divulgation dans les affaires criminelles :*** La Cour suprême a depuis longtemps établi l'obligation de la Couronne de communiquer tous les renseignements pertinents et substantiels, qui ne sont pas confidentiels, à la défense afin que les accusés puissent

79 *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21.
80 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5.
81 *R. c. Spencer*, 2014 CSC 43.
82 *R. c. Bykovets*, 2024 CSC 6.

présenter une défense pleine et entière aux accusations portées contre eux[83]. Cependant, cette obligation légale de divulgation peut représenter une difficulté dans le contexte des enquêtes criminelles sur la sécurité nationale, un problème généralement connu sous le nom de dilemme de la conversion des renseignements en preuve[84]. Ce dilemme se pose particulièrement dans les circonstances où un outil ou une technique sensible partagé a été utilisé pour recueillir des éléments de preuve, comme des messages texte entre des suspects qui planifieraient une attaque.

L'approche du Canada en matière de capacité d'interception

49. Dans le contexte de l'accès légal, l'interception de communications privées, comme les appels téléphoniques et les courriels, exige souvent la collaboration d'un ou de plusieurs FSC. Les FSC sont des entités qui offrent des services de télécommunications ou une certaine combinaison de services d'information et de médias, de contenu, de divertissement et d'applications sur des réseaux[85]. Pour exécuter un mandat du SCRS ou de la GRC, certains FSC comptent sur des outils intégrés à leur système ou réseau de télécommunications pour intercepter les communications ou d'autres données.

50. À l'heure actuelle, il n'existe aucun mécanisme législatif au Canada obligeant les FSC à concevoir, à déployer ou à maintenir leurs systèmes de façon à demeurer en mesure de réaliser des interceptions. Cela signifie que même si les organismes d'application de la loi ou les responsables de la sécurité nationale obtiennent une autorisation judiciaire préalable pour intercepter les communications d'une cible particulière, ils pourraient ne pas être en mesure d'obtenir ces communications parce qu'il n'existe pas de solution technologique pour intercepter, recueillir et transférer les communications ou leurs données connexes à l'organisme demandeur[86].

51. Il existe une exception notable, bien que datée. En vertu des *Normes d'application du Solliciteur général sur l'interception licite des télécommunications*, certains FSC doivent veiller à ce que leurs systèmes puissent réaliser des interceptions en vue d'obtenir une licence au titre de la *Loi sur la radiocommunication*. Mises à jour en 1995, ces normes ne s'appliquent qu'aux radiofréquences pour les services de téléphonie vocale sans fil, c'est-à-dire les services de téléphonie cellulaire[87]. Elles ne s'appliquent pas aux téléphones filaires ni aux technologies de communication numérique comme le courriel, les médias sociaux et les plateformes de messagerie, les communications par satellite ou le Wi-Fi. Ces normes n'ont pas force de loi et tous les fournisseurs de services cellulaires ne s'y conforment pas entièrement[88].

52. Le Canada fait figure d'exception parmi les autres pays du Groupe des cinq et du Groupe des Sept, qui ont tous adopté des lois obligeant les FSC à maintenir des réseaux aptes à l'interception. En 2023, la GRC a mené une analyse comparative d'autres démocraties occidentales, examinant l'Allemagne, l'Australie, la Belgique, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, l'Irlande, la Norvège, la Nouvelle-Zélande, les Pays-

83 *R. c. Stinchcombe*, [1991] 3 RCS 326.
84 Craig Forcese et Leah West, *National Security Law*, 2020.
85 Lawful Access Advisory Committee, « Governance Framework », mai 2024.
86 Industrie Canada, ministère de la Justice et Solliciteur général Canada, *Accès légal – Document de consultation*, 2002.
87 Lawful Access Advisory Committee, « Governance Framework », mai 2024.
88 Sécurité publique Canada, comparution devant le CPSNR, 11 avril 2024.

Bas, le Royaume-Uni, la Suède et la Suisse. Quand bien même chaque pays posséderait un cadre distinct, ils disposent tous d'une législation régissant la capacité d'interception[89]. La loi de certains pays s'applique seulement aux services de communication traditionnels comme la téléphonie filaire et mobile et les fournisseurs de services Internet, alors que la loi d'autres pays s'applique tant aux services traditionnels que modernes (p. ex., les exploitants de réseaux virtuels mobiles et les applications par contournement). Pour ce qui est du modèle de financement des coûts associés à la conception et à l'entretien de la capacité d'interception, les pays avaient adopté différents modèles et frais d'exploitation, c'est-à-dire un modèle où les FSC assumaient les coûts, un autre où le gouvernement assumait les coûts ou encore un modèle où les coûts étaient partagés entre les FSC et le gouvernement[90]. Le tableau 2.1[91] résume les positions des partenaires dans le Groupe des cinq concernant des éléments clés de la capacité d'interception.

89 GRC, « International Comparison of Lawful Access Coordination and Funding Models », ébauche, 2023.
90 GRC, « International Comparison of Lawful Access Coordination and Funding Models », ébauche, 2023.
91 Adapté d'une présentation de Sécurité publique Canada. Le CPSNR a ajouté la rangée intitulée *Couverture* et la colonne *Canada*. Sécurité publique Canada, comparution devant le CPSNR, 11 avril 2024. Dans ce contexte, le Comité entend par « entreprise de télécommunication » un exploitant d'une installation de transmission grâce à laquelle sont fournis par lui-même ou une autre personne des services de télécommunication au public moyennant contrepartie.

Tableau 2.1 : Législation régissant la capacité d'interception au Canada, au Royaume-Uni, en Australie, aux États-Unis et en Nouvelle-Zélande

	CANADA	ROYAUME-UNI	AUSTRALIE		ÉTATS-UNIS	NOUVELLE-ZÉLANDE
Loi	Aucun(e)	*Investigatory Powers Act 2016* (modifications en 2024)	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*	*Telecommunications (Interception and Access) Act 1979* (dernière mise à jour en 2021)	*Communications Assistance for Law Enforcement Act* (CALEA)	*Telecommunication (Interception Capability and Security) Act 2013*
Application		Tous les FSC	Tous les FSC	Entreprises de télécommunications	Entreprises de télécommunications	Entreprises de télécommunications
Exigence		Le ministre oblige individuellement les FSC à concevoir et à entretenir une capacité d'interception par des décrets.	Les organismes pourraient avoir besoin d'aide et les ministres pourraient demander que des capacités soient mises au point.	Exigences générales relatives à la capacité d'interception.	Exigences générales relatives à la capacité d'interception.	Exigences générales relatives à la capacité d'interception.
Couverture		Couverture complète Contrairement aux États-Unis ou à la Nouvelle-Zélande, les lois du Royaume-Uni et de l'Australie en matière d'interception s'appliquent aux plateformes de médias sociaux et applications de messagerie à l'extérieur du pays.			Couverture partielle : La CALEA s'applique aux téléphones filaires et cellulaires, aux messages texte, au service Internet à large bande et à la voix sur protocole Internet.	Couverture complète pour les entreprises de télécommunications seulement.
Cadre d'indemnisation		Le gouvernement doit verser une « contribution appropriée » en prévision des coûts liés au respect de la loi.	Les fournisseurs sont habituellement indemnisés pour les coûts raisonnables liés au respect de la loi.	Les FSC assument les coûts de la capacité d'interception.	Une indemnisation peut être versée si la capacité n'est pas « facilement réalisable ».	Les FSC assument les coûts de la capacité d'interception.

Transparence et examen

53. Sur le plan de l'accès légal, les organismes d'application de la loi et de sécurité du Canada sont assujettis à diverses obligations en matière de divulgation, de transparence et d'examen. En ce qui concerne la GRC, le gouvernement est tenu de faire rapport annuellement au Parlement sur l'utilisation de la surveillance électronique audio et vidéo[92]. Le gouvernement a déposé son plus récent rapport au Parlement, le *Rapport annuel sur la surveillance électronique 2020*, en 2022[93].

54. Le SCRS n'est pas tenu de déclarer publiquement le nombre d'enquêtes qu'il mène ni son utilisation de la surveillance électronique. De même, le CST n'est pas tenu de déclarer publiquement le nombre de demandes d'assistance qu'il reçoit du SCRS et de la GRC ou auxquelles il répond.

55. Les trois organisations sont assujetties à l'examen par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et par le présent Comité.

92 *Code criminel*, L.R.C. (1985), ch. C-46, art. 195; et GRC, « RCMP factual accuracy submission – NSICOP Lawful Access Draft Report », 20 décembre 2024.

93 Sécurité publique Canada, *Rapport annuel sur la surveillance électronique - 2022*, mai 2024. Le rapport porte sur une période de cinq ans entre 2018 et 2022.

Chapitre 3 : Défis de l'accès légal

56. Les organismes de sécurité et de renseignement du Canada déclarent éprouver de grandes difficultés à obtenir un accès légal aux communications en raison du fossé qui se creuse entre l'autorisation légale de recueillir des informations et la capacité technique de le faire[94]. En 2018, le directeur du Service canadien du renseignement de sécurité (SCRS) a décrit les problèmes d'accès légal comme l'un des « défis les plus importants » qu'il avait soulevés au gouvernement[95]. La situation s'explique par trois facteurs : les répercussions des avancées technologiques, l'absence d'une législation régissant la capacité d'interception, et les défis sur le plan des compétences découlant de la nature transfrontalière des données numériques. Le présent chapitre décrit ces défis, ainsi que leurs répercussions sur la capacité de la Gendarmerie royale du Canada (GRC) et du SCRS à mener des enquêtes sur la sécurité nationale, et la façon dont ces organisations se sont adaptées pour atténuer ces difficultés. Tout au long du chapitre, les opinions d'experts en cybersécurité et en droit, de défenseurs de la vie privée et de représentants de l'industrie sont présentées.

Les répercussions des avancées technologiques

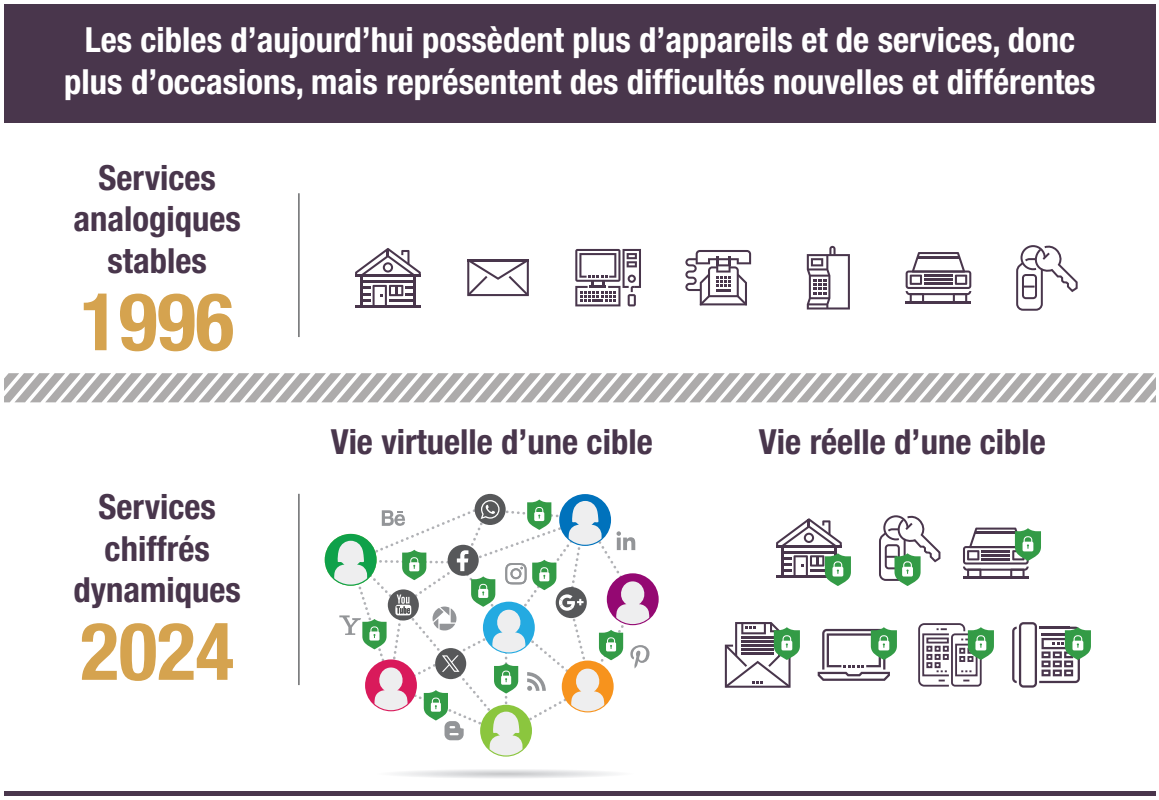
57. Selon l'experte en cybersécurité Susan Landau, l'humanité se trouve au milieu d'une révolution numérique, une période où la société humaine vit une transformation aussi importante que lors des révolutions agricole et industrielle qui l'ont précédée, mais à un rythme supérieur et entraînant des conséquences plus profondes[96]. L'introduction du microprocesseur, l'ouverture d'Internet à des fins commerciales, l'adoption rapide des téléphones cellulaires et leur évolution en téléphones intelligents, et l'avènement des médias sociaux et du courrier Web, parmi les nombreuses autres avancées, ont radicalement transformé le quotidien des humains. L'intelligence artificielle accélérera probablement ce rythme de changement déjà exponentiel.

58. L'adoption répandue des technologies numériques a aussi transformé la façon dont les organismes de renseignement et d'application de la loi mènent leurs enquêtes sur les menaces envers la sécurité nationale. Selon Sécurité publique Canada, même si ces avancées technologiques offrent plus de possibilités d'interception, elles présentent de nouveaux et différents défis pour les professionnels de la sécurité nationale, comme le montre la figure 3.1[97]. D'après le SCRS et la GRC, ce nouvel environnement est de plus en plus complexe pour plusieurs raisons clés[98].

94 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
95 Stephanie Carvin et Craig Forcese, « Episode 36: An INTREPID Podsight: CSIS Director David Vigneault », 11 mai 2018.
96 Susan Landau, *Listening In: Cybersecurity in an Insecure Age*, Yale University Press, 2017.
97 Sécurité publique Canada, « Les changements technologiques et leurs répercussions politiques sur l'accès légal : Exposé d'établissement de la portée au Comité des parlementaires sur la sécurité nationale et le renseignement », 11 avril 2024.
98 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.

59. Premièrement, les Canadiens disposent de plus de façons de communiquer que jamais auparavant, y compris plus d'appareils, plus de services et plus de fournisseurs[99]. Par conséquent, la quantité, la variété et la vélocité des données générées sont plus grandes que par le passé. Au nombre des types de données, mentionnons les communications vocales, les historiques de recherche sur Internet, les transcriptions de clavardage et la géolocalisation, créant une profusion de métadonnées, soit des « données sur des données[100] ». Divers objets Web « intelligents » utilisés couramment, comme des moniteurs d'activité physique personnels, des télévisions et des automobiles, sont maintenant munis de capteurs intégrés, de composants électriques et de logiciels qui recueillent des données et de l'information dans l'environnement où ils se trouvent, alimentant l'abondance de métadonnées. Selon le Centre canadien pour la cybersécurité (CCC), décrivant le phénomène comme l'Internet des objets, plus de 30 milliards de dispositifs y seront connectés d'ici 2025[101].

Figure 3.1 : L'accès légal, d'hier à aujourd'hui[102]



99 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.

100 Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, document commandé par le CPSNR, 30 août 2023.

101 Centre canadien pour la cybersécurité (CCC), « Sécurité de l'Internet des objets (IdO) – ITSAP.00.012 », juillet 2022.

102 Adaptée de Sécurité publique Canada, « Les changements technologiques et leurs répercussions politiques sur l'accès légal », 11 avril 2024.

60. Deuxièmement, il est de plus en plus facile de protéger le contenu des communications grâce à l'utilisation répandue du chiffrement, qui est le processus de conversion de l'information numérique dans un format illisible, de façon à ce que seule une personne détenant la clé de déchiffrement puisse la lire. Le chiffrement est employé pour authentifier les utilisateurs et maintenir la confidentialité de l'information, protégeant ainsi les « données au repos » et les « données en transit »[103]. Considéré largement comme une pratique exemplaire visant à accroître la sécurité et à protéger la vie privée en ligne, le chiffrement est un élément vital de la cybersécurité, du commerce électronique, de la protection des données et de la propriété intellectuelle, et des intérêts commerciaux[104]. Selon le SCRS, 90 % du trafic Internet est chiffré[105].

61. Au cours de la dernière décennie, l'adoption d'applications et de services de communication par contournement offrant un chiffrement de bout en bout (comme WhatsApp ou Telegram) connaît une hausse. Donc, malgré la mise en place d'une solution avec un FSC, l'utilisation d'applications chiffrées de bout en bout limite la capacité des organismes d'application de la loi et de sécurité de lire les messages du destinataire visé, car ni le fournisseur de service de messagerie ni l'entreprise de télécommunications ne peut déchiffrer les messages. Outre les technologies de chiffrement, la prédominance de technologies d'anonymisation, comme les réseaux privés virtuels (RPV), The Onion Router et le Web clandestin, rend difficile ***[106]. Pour ce que l'avenir réserve, l'évolution de l'intelligence artificielle et l'adoption prévue de l'informatique quantique ajouteront une couche supplémentaire de complexité (voir l'encadré).

> Selon le CCC, le **Web clandestin** est un segment non indexé d'Internet qui est seulement accessible au moyen d'un logiciel spécialisé ou de mandataires réseau comme The Onion Router. Cet accès sert principalement à masquer l'identité de l'utilisateur : « [e]n raison de sa nature axée sur l'anonymat et la confidentialité, le Web clandestin facilite un écosystème complexe de cybercriminalité et de commerce de biens et de services illicites[107]. »

62. Troisièmement, la nature transnationale d'Internet signifie que les flux transfrontaliers des données représentent la règle plutôt que l'exception. Le cyberespace n'est pas limité par des frontières géopolitiques. De nombreux Canadiens, voire la majorité d'entre eux, utilisent des services numériques dont les solutions de messagerie proviennent d'entreprises tierces établies à l'extérieur du Canada.

> Selon le CST, les **ordinateurs quantiques** constituent une menace à venir pour la cybersécurité. Conçus pour exploiter la physique quantique pour résoudre des problèmes computationnels beaucoup plus rapidement que les ordinateurs actuels, ils rendent facilement obsolètes les méthodes de cryptographie actuelles[108]. Alors que l'arrivée d'ordinateurs

103 Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, publication de recherche commune par le Citizen Lab de l'Université de Toronto et la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa, 2018.
104 Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale, 2016*, 2016.
105 SCRS, comparution devant le CPSNR, 13 juin 2024.
106 ***.
107 CCC, *Évaluation des menaces de base : Cybercriminalité*, août 2023; et FBI, « A Primer on DarkNet Marketplaces », novembre 2016.
108 Centre de la sécurité des télécommunications (CST), « CSE Comments on NSICOP's Draft Lawful Access Report », 20 décembre 2024.

quantiques suffisamment puissants pour déchiffrer toutes les clés de chiffrement actuelles n'est pas prévue avant la prochaine décennie, les auteurs de menace pourraient stocker des informations chiffrées en vue de les déchiffrer éventuellement.

Les répercussions des nouvelles technologies sur les enquêtes sur la sécurité nationale

63. D'après le SCRS, le plus grand obstacle à l'exécution de son mandat [traduction] « sur le plan de sa capacité de détecter et d'atténuer les menaces est le changement technologique rapide qui dépasse ses autorisations et ses outils[109]. » Le SCRS et la GRC affirment tous deux que les techniques d'interception traditionnelles servant à la collecte de communications sont devenues de moins en moins utiles à mesure que le chiffrement s'est répandu, ce qui aide les auteurs de menace à ne pas être découverts et faire l'objet d'enquêtes et de poursuites, ***[110]. Le SCRS et la GRC ajoutent que ces technologies ont posé d'importantes difficultés pour les enquêtes sur le terrorisme, l'espionnage, l'ingérence étrangère et le crime organisé[111].

64. Ni le SCRS ni la GRC ne recueille systématiquement de données sur le nombre d'enquêtes sur la sécurité nationale comportant un élément de chiffrement. Cela dit, une étude moins récente de la GRC fait exception. Elle portait sur les difficultés technologiques de l'obtention d'éléments de preuve numériques autorisés judiciairement dans ses 57 enquêtes majeures de la Police fédérale actives en 2014, dont 25 étaient des enquêtes sur la sécurité nationale. Toutes les enquêtes ont comporté des difficultés sur le plan technologique dans l'acquisition d'éléments de preuve autorisés judiciairement, mais aucune n'a été close pour cette raison. ***[112]. La GRC n'a réalisé aucune autre étude de ce genre depuis. Devant le Comité, le SCRS a souligné la difficulté de quantifier les réussites et les échecs pour ce qui est de surmonter les défis du chiffrement, tandis que Sécurité publique Canada a indiqué que les organismes de sécurité parviennent facilement à trouver des solutions de rechange[113].

65. Le SCRS indique aussi que même si les nouvelles technologies et les nouveaux types de données présentent des possibilités de collecte de renseignements, les défis l'emportent sur les avantages, puisqu'il existe trop d'applications et de types d'appareils pour rester à jour[114]. ***[115].

109 SCRS, comparution devant le CPSNR, 13 juin 2024.
110 SCRS, « Summary of Workshop on Intercept Capability and Encryption », sans date; SCRS, comparution devant le CPSNR, 28 mai 2024; et GRC, comparution devant le CPSNR, 30 mai 2024.
111 SCRS, comparution devant le CPSNR, 13 juin 2024.
112 ***
113 Sécurité publique Canada et SCRS, comparution devant le CPSNR, 5 novembre 2024.
114 SCRS, comparution devant le CPSNR, 13 juin 2024.
115 SCRS, comparution devant le CPSNR, 18 avril 2024.

Étude de cas : *

***[116]. ***[117]. ***

Pour faire enquête sur cette menace envers la sécurité du Canada aux termes de l'article 12 de la Loi sur le SCRS, le Service a obtenu une série de mandats en vertu de l'article 21 de sa loi habilitante. ***[118]

***[119]. ***[120]

***[121]. ***[122]. ***

***[123] ***[124]

66. Alors que les cibles de la sécurité nationale choisissent des applications chiffrées de bout en bout et des réseaux privés virtuels pour dissimuler leurs activités, la GRC et le SCRS ont indiqué au Comité ***, une difficulté exacerbée par de récentes décisions judiciaires[125]. Le SCRS et la GRC se servent des renseignements de base sur les abonnés (RBA) pour déterminer qui se cachent derrière un identifiant numérique (c'est-à-dire une adresse de protocole Internet) en vue d'enquêter sur des menaces possibles. Comme l'indique le chapitre 2, compte tenu de la décision de la Cour suprême en 2014 dans l'affaire *Spencer* voulant que les organismes de sécurité doivent posséder une autorisation judiciaire pour obtenir des RBA, le SCRS et la GRC doivent prendre des mesures additionnelles pour accéder à ce qu'ils considéraient être des renseignements constitutifs des premières étapes d'une enquête. D'après le SCRS, l'exigence relative à l'autorisation judiciaire pour l'obtention de ce type de renseignements entraîne des retards et demande au SCRS de déployer des efforts importants pour enquêter sur une menace possible, d'autant plus qu'il cherche à écarter des personnes afin que les enquêteurs puissent se concentrer sur les réels auteurs de menace. Les partenaires du Canada membres du Groupe des cinq n'ont pas à posséder une autorisation judiciaire pour obtenir des RBA[126].

67. La GRC affirme qu'il est aussi difficile pour elle d'exploiter au maximum les métadonnées qu'elle saisit, précisant que la quantité astronomique de données liées aux métadonnées, qui ne sont en majorité pas pertinentes, peut submerger les enquêteurs[127]. En outre, il n'existe aucune exigence légale obligeant les FSC à conserver certaines métadonnées pour une

116 ***
117 SCRS, *Rapport annuel 2023-2024 sur les activités opérationnelles présenté au ministre conformément au paragraphe 6(4) de la Loi sur le SCRS*, 2024.
118 SCRS, « Response to RFI #4 », 13 novembre 2024.
119 SCRS, exposé devant le Secrétariat du CPSNR, 10 décembre 2024; et SCRS, « Factual accuracy check of the case study », fourni au CPSNR à sa demande le 8 janvier 2024.
120 SCRS, exposé devant le Secrétariat du CPSNR, 10 décembre 2024.
121 SCRS, exposé devant le Secrétariat du CPSNR, 10 décembre 2024.
122 Michael Geist, *Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes Internet*, document commandé par le CPSNR, mai 2024.
123 SCRS, *Rapport annuel 2023-2024 sur les activités opérationnelles présenté au ministre conformément au paragraphe 6(4) de la Loi sur le SCRS*, 2024.
124 ***
125 SCRS, comparution devant le CPSNR, 28 mai 2024.
126 SCRS, comparution devant le CPSNR, 28 mai 2024.
127 GRC, comparution devant le CPSNR, 13 juin 2024. Voir aussi CPSNR, *Rapport spécial sur le mandat de la Police fédérale de la Gendarmerie royale du Canada*, chapitre 5, 2023; et SCRS, « Summary of Workshop on Intercept Capability and Encryption », sans date.

période donnée[128]. Par conséquent, même si la GRC ou le SCRS pouvait demander une ordonnance de conservation pour forcer un fournisseur à conserver des données précises, les enquêteurs pourraient découvrir que le fournisseur a déjà supprimé les données avant de recevoir l'ordonnance en raison de ses propres politiques de gestion des données. Selon la GRC, l'absence d'un régime entourant la conservation des données entraîne des conséquences considérables étant donné que certaines enquêtes complexes durent des années, tandis que d'autres enquêtes commencent des années après la création initiale des données[129].

La ***conservation des données*** renvoie à une exigence légale générale obligeant les FSC à conserver certaines métadonnées pour une période précise. Il n'existe aucune loi au Canada prévoyant de telles dispositions[130].

La ***préservation des données*** renvoie à des dispositions de la Loi sur le SCRS et du *Code criminel* qui permettent aux enquêteurs d'obliger une personne ou une entité à préserver des données qu'elles auraient autrement supprimées (c'est-à-dire en raison de sa pratique ou de sa politique organisationnelle habituelle). Les ordres et les ordonnances de préservation sont délivrés dans l'optique que l'enquêteur obtiendra un mandat ou une ordonnance de communication en vue d'obtenir les données en soi. Dans le *Code criminel*, un ordre de préservation permet à un agent de la GRC d'obliger la préservation sans autorisation judiciaire[131]. La Loi sur le SCRS ne prévoit aucun ordre de préservation. Les ordonnances de préservation, prévues dans la Loi sur le SCRS[132] et le *Code criminel*[133], exigent une autorisation judiciaire.

68. Les défenseurs de la vie privée affirment que les métadonnées représentent une source d'information précieuse, souvent non chiffrée, pour les enquêteurs qui a peut-être été sous-exploitée[134]. Selon le Citizen Lab, le SCRS et la GRC ne perdent pas accès à l'information. Plutôt, une « friction » gêne leurs enquêtes et ils doivent développer leur expertise, augmenter leurs dépenses et redoubler d'ingéniosité pour enquêter sur les menaces à la sécurité nationale[135]. Les défenseurs de la vie privée indiquent également que les organisations du secteur privé recueillent de grands ensembles de renseignements personnels possiblement révélateurs dans le cadre de la « surveillance commerciale » générale[136], donnant l'occasion aux organismes de sécurité et de renseignement de recueillir de l'information. Ils soutiennent aussi que [traduction] « nous sommes loin de "nous retrouver dans le noir", car il y a beaucoup plus d'informations disponibles sur la vie privée des personnes aujourd'hui qu'à n'importe quelle époque[137]. »

128 Ministère de la Justice, comparution devant le CPSNR, 7 novembre 2024; et gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016 : Document de contexte*, 2016.
129 GRC, « Lawful Access in Canada: Examining the challenges of lawfully accessing communications data in a digital world », ébauche, 2023.
130 Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale, 2016*, 2016.
131 *Code criminel*, L.R.C. (1985), ch. C-46, article 487.012.
132 Loi sur le SCRS, L.R.C. (1985), ch. C-23, article 20.3.
133 *Code criminel*, L.R.C. (1985), ch. C-46, article 487.013.
134 Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
135 Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
136 BCCLA, comparution devant le CPSNR, 1er octobre 2024.
137 Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.

69. Le SCRS proteste qu'il n'est pas en mesure d'accéder à ces données ou de les recueillir étant donné les limites actuelles du Canada sur le plan technologique et légal. Les entités commerciales qui recueillent ces données sont principalement situées à l'extérieur du Canada (les défis sur le plan des compétences sont traités plus loin dans le présent chapitre)[138]. Le SCRS souligne également que l'État ne peut recueillir l'information disponible à tous sur Internet, comme les adresses IP, sans autorisation judiciaire en raison des décisions de la Cour suprême dans les affaires *Spencer* et *Bykovets*[139].

70. Les experts en droit à la vie privée soulignent également que les organismes de sécurité exagèrent les obstacles qu'ils doivent franchir :

> [l]e stockage numérique est si abordable aujourd'hui que n'importe quelle donnée recueillie pour une enquête peut être conservée indéfiniment. De plus, les outils numériques tels que la reconnaissance vocale, la traduction automatique et les analyses alimentées par l'intelligence artificielle peuvent éplucher automatiquement pour les organismes gouvernementaux des tonnes de données numériques interceptées et relever les éléments qui vaudraient la peine d'être analysés par leur personnel[140].

71. Le SCRS avance que la réalité est plus complexe, soulignant que ses mandats lui imposent des restrictions strictes qui précisent les périodes de conservation des données recueillies (c'est-à-dire que le SCRS ne peut pas conserver indéfiniment les données) et des exigences indiquant que les données doivent être examinées par des employés désignés du SCRS (c'est-à-dire non pas par un programme automatisé)[141].

72. Se penchant sur les prémisses du débat de 2011 soutenant que les gouvernements vivaient dans un « âge d'or de la surveillance », le SCRS indique qu'à l'époque, les communications sur Internet étaient plus vulnérables que les appels téléphoniques traditionnels, à moins d'être chiffrées, et que, même alors, les organismes d'application de la loi indiquaient avoir été en mesure d'extraire les communications lisibles dans les rares cas où ils ont fait face à cette situation[142]. Or, le SCRS déclare que cette situation a grandement changé, car le trafic Internet est désormais majoritairement chiffré par défaut ***[143].

138 SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.
139 SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.
140 Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, document commandé par le CPSNR, 30 août 2023.
141 SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.
142 SCRS, citant Peter Swire et Kenesa Ahmad, « Encryption and Globalization », *Columbia Science and Technology Law Review, Vol. 23, 2012*, 17 novembre 2011.
143 SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.

Pallier les difficultés des nouvelles technologies dans le milieu de la sécurité nationale

73. Selon le SCRS et la GRC, pour pallier les difficultés technologiques, ils doivent mener des activités qui exigent beaucoup de ressources et comportent des risques opérationnels plus importants[144]. ***[145].

74. On compte parmi les efforts visant à pallier les difficultés technologiques des investissements croissants dans les moyens de collecte de renseignements *** et dans les opérations de sources humaines en vue de recueillir des informations sur des sujets d'enquête visés par un mandat[146]. L'augmentation du nombre d'opérations *** « qui sont risquées, qui exigent des efforts considérables et qui sont coûteuses ***[147] » représente aussi un autre moyen d'atténuation. ***[148].

L'exploitation de réseau informatique et l'utilisation d'outils d'enquête sur appareil

75. L'une des principales méthodes qu'ont employées le SCRS et la GRC pour contourner la difficulté découlant des technologies de chiffrement au cours de la période à l'examen était l'exploitation de réseau informatique (ERI)[149]. L'ERI renvoie aux outils et techniques qui exploitent les vulnérabilités dans les systèmes ou logiciels pour obtenir subrepticement des données stockées ou passant dans des réseaux de communication ***. La GRC utilise le terme « outil d'enquête sur appareil » (OEA) ou « outil d'enquête embarqué » (OEE) pour décrire ses outils d'ERI[151]. Un OEA est « un programme informatique au sens [du paragraphe] 342.1(2) du *Code criminel*, installé sur un dispositif informatique ciblé et qui permet de recueillir des preuves électroniques sur ce dispositif[152]. » ***

> *** ce programme de collecte technique est toutefois l'un des plus complexes et coûteux actuellement en activité[153].

76. Lorsque suffisamment de vulnérabilités ont été cernées, l'ERI permet *** à la GRC de recueillir des informations directement du téléphone intelligent ou de l'ordinateur d'une personne ciblée et elle permet aux enquêteurs d'accéder non seulement aux appels et messages texte du cellulaire de la personne, mais aussi *** ses courriels, messages chiffrés ***[154]. L'ERI peut aussi permettre aux enquêteurs d'activer le microphone ou la caméra du téléphone de la personne visée[155]. L'étude de cas ci-dessous présente un exemple d'enquête dans le cadre de laquelle la GRC a réussi à déployer des OEA pour faire face à une menace envers la sécurité nationale.

144 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
145 ***
146 SCRS, comparution devant le CPSNR, 28 mai 2024.
147 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024; et SCRS, comparution devant le CPSNR, 28 mai 2024.
148 SCRS, comparution devant le CPSNR, 28 mai 2024.
149 Témoignage du commissaire de la GRC devant 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), *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*, novembre 2022; et SCRS, comparution devant le CPSNR, 28 mai 2024.
150 ***
151 GRC, réponse du gouvernement à la demande de renseignements du gouvernement Q-566, 6 mai 2022.
152 GRC, « Outils d'enquête embarqués (OEE) – Description technique : Ébauche du Projet », août 2022.
153 ***
154 ***
155 ***

Étude de cas : Projet SALENTO de la GRC

***, le Federal Bureau of Investigation (FBI) des États-Unis a transmis des renseignements à la GRC au sujet d'un Canadien (l'individu) ***[156] ***[157]. La GRC a enquêté sur l'individu tout au long de 2018, dans le cadre d'une enquête criminelle appelée Projet SALENTO[158]. ***[159].

*** de l'individu : ***[160] qui aurait été en train de fabriquer une bombe en vue de perpétrer un attentat terroriste au Canada, ciblant des festivités du Nouvel An du 31 décembre. ***[161].

En réponse, la GRC a pris de nombreuses mesures d'enquête, y compris le déploiement d'OEA sur les appareils de l'individu et ***. Les OEA ont révélé des messages texte et des schémas d'une bombe dans un autocuiseur[162].

Le 24 janvier 2019, la GRC a arrêté *** à Kingston, en Ontario[163]. Quatre chefs d'accusation pour terrorisme ont été portés contre ***, auxquels il a plaidé coupable le 28 juillet 2020[164]. Les éléments de preuve recueillis par les OEA ont étayé les accusations portées. Selon la GRC, l'utilisation fructueuse d'OEA dans le Projet SALENTO peut être attribuée à plusieurs facteurs clés. Tout d'abord, la GRC disposait déjà d'une capacité pour déployer un OEA pour le modèle et le fabricant des téléphones utilisés par l'individu et ***, ce qui n'est pas toujours le cas[165]. ***

77. Bien que le SCRS et la GRC emploient tous deux des outils d'ERI dans le cadre d'enquêtes sur la sécurité nationale, le CST joue un rôle principal dans la gestion des politiques entourant l'ERI et sa mise en œuvre pour le gouvernement. Plus particulièrement, le CST gère l'exploitation des vulnérabilités de systèmes et de logiciels, connues aussi sous le nom de « nouvelles capacités », par l'entremise du Cadre de gestion du partage des nouvelles capacités, qui fournit un « processus décisionnel normalisé permettant à des spécialistes du CST d'étudier l'information disponible dans le but d'assurer une gestion responsable des nouvelles capacités associées à une vulnérabilité relevée dans un système d'information ou dans une technologie, tout en considérant la sécurité du Canada et des Canadiennes et Canadiens comme la principale priorité[166]. » Le SCRS et la GRC font partie du Comité de révision des nouvelles capacités prévu dans le Cadre de gestion du partage des nouvelles capacités. ***[167].

156 ***
157 ***
158 À la GRC, une enquête criminelle majeure porte le nom de projet.
159 ***
160 ***
161 ***
162 Voir, par exemple, deux rapports complémentaires de la salle d'interception de la GRC datés du 2 janvier 2019 (rapports nº 00006710 et 00006711), et le fichier de la GRC intitulé « Images captured by ODIT – 00014169 ».
163 Canadian Broadcasting Corporation (CBC), « RCMP charge Kingston, Ont. youth with terror-related offence after security probe », 25 janvier 2019; et SPPC, « Adolescent plaide coupable à quatre infractions de terrorisme », 28 juillet 2020.
164 SPPC, « Adolescent plaide coupable à quatre infractions de terrorisme », 28 juillet 2020.
165 GRC, exposé devant le Secrétariat du CPSNR, 27 novembre 2024.
166 ***
167 ***

78. Tant pour le SCRS que la GRC, l'obtention d'une autorisation judiciaire en vue de l'utilisation de l'ERI peut être complexe en fonction de l'objectif de l'activité. La GRC requiert plusieurs autorisations, notamment pour l'écoute électronique si l'OEA sert à intercepter des communications privées, ainsi qu'un mandat général et un mandat d'enregistreur de données de transmission[168]. ***[169] ***[170] ***[171].

79. Le SCRS indique que les mandats autorisant l'installation et l'utilisation d'OEA contiennent plusieurs mesures de protection en matière de vie privée, à l'instar de ses politiques internes, ***[172] ***[173] ***[174].

80. D'après le SCRS, il a commencé en 2018 à fournir à la Cour fédérale une explication sur le fonctionnement de ses OEA et leurs différentes méthodes de déploiement dans ses demandes de mandat afin que les juges désignés [traduction] « reçoivent des informations uniformes sur les pouvoirs liés aux OEA qu'ils autoriseraient[175] ».

81. Les mandats délivrés à la GRC pour le déploiement d'OEA visant à intercepter des communications privées incluent aussi des mesures de protection de la vie privée. Le juge qui délivre un mandat peut imposer des modalités à l'autorisation d'écoute électronique[176], comme des restrictions sur les sujets et les catégories qui peuvent être recherchés dans les données extraites de l'appareil, ou des exigences en vue de détruire les données recueillies qui ne correspondent pas à la période autorisée ou de mettre fin à l'examen de données qui ne se rapportent pas à une cible[177].

82. *** la GRC déploient l'ERI de trois différentes manières, ***[178] :

1. *ERI par accès à distance* : ***
2. *ERI par accès proche* : ***[179].
3. *ERI par accès direct* *** : ***[180].

83. L'ERI n'est pas une solution miracle. Elle repose sur l'exploitation de vulnérabilités ***. Au cours des dernières années, le nombre d'appareils et d'applications a fait augmenter le coût et la complexité de l'ERI, car les opérateurs doivent élargir leurs recherches à plus d'appareils et applications pour trouver leurs vulnérabilités[181] ***[182] ***[183]

168 GRC, « Outils d'enquête embarqués (OEE) – Description technique : Ébauche du Projet », août 2022.
169 ***
170 ***
171 ***
172 SCRS, réponse à « Inconsistencies between CSIS RFI #4 Response (Nov. 14/24) and CSIS Factual Accuracy Response (Dec. 20, 2024) », 6 janvier 2024.
173 *** SCRS, réponse à « Inconsistencies between CSIS RFI #4 Response (Nov. 14/24) and CSIS Factual Accuracy Response (Dec. 20, 2024) », 6 janvier 2024.
174 SCRS, « CSIS Response to NSICOP RFI #4 on Lawful Access », 13 novembre 2024.
175 SCRS, « CSIS Response to NSICOP RFI #4 on Lawful Access », 13 novembre 2024; et SCRS, « CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review », 20 décembre 2024.
176 *Code criminel*, L.R.C. (1985), ch. C-46, paragraphe 186(3) ou alinéa 186(4)d).
177 Cour supérieure de justice des tribunaux de l'Ontario (région de l'Est), « Authorization to intercept communications, make observations, and related orders and warrants », 3 janvier 2019.
178 ***
179 ***
180 ***
181 GRC, comparution devant le CPSNR, 30 mai 2024.
182 ***
183 ***

84. ***[184]

85. ***[185] ***[186] ***

***[187]

86. En 2022, la GRC a indiqué au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) que, depuis 2017, elle avait eu recours aux OEA dans 32 enquêtes, ciblant 49 dispositifs[188]. Depuis, la GRC a tenté à huit reprises de déployer un OEA en 2023, et seuls deux déploiements ont été fructueux. La GRC n'a pas déployé d'OEA en 2024[189]. De même, la GRC a indiqué que la sensibilisation accrue à la cybersécurité au cours des dernières années a entraîné une baisse considérable de son taux de réussite global des OEA[190]. Le tableau 3.2 résume le nombre d'OEA déployés par la GRC depuis 2007.

Tableau 3.2 : Utilisation d'OEA par la GRC, 2017-2024[191]

ANNÉE	NOMBRE D'APPAREILS CIBLÉS	DÉPLOIEMENTS FRUCTUEUX
2017	2	2
2018	3	3
2019	2	2
2020	15	8
2021	16	9
2022	11	7
2023	8	2
2024	0	0

Le Comité comprend que, pour le SCRS et la GRC, un déploiement d'OEA fructueux signifie qu'un OEA a recueilli de l'information sur l'appareil ciblé et a créé un rapport, ***[192].

184 SCRS, ***
185 *** SCRS, « CSIS Response to NSICOP RFI #4 on Lawful Access », 13 novembre 2024.
186 SCRS, « CSIS Response to NSICOP RFI #4 on Lawful Access », 13 novembre 2024.
187 ***
188 GRC, *Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur l'étude des outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada*, août 2022.
189 GRC, « RCMP Response to NSICOP's Review of the Lawful Access to Communications by Security and Intelligence Organizations (RFI #05) », 14 novembre 2024.
190 SCRS, comparution devant le CPSNR, 13 juin 2024; et GRC, comparution devant le CPSNR, 30 mai 2024.
191 GRC, « RFI #7 Chart », 18 décembre 2024; et GRC, « RE: [NEW RFI] NSICOP lawful access report – verification request », 4 février 2025. La GRC a signalé qu'elle ne tente habituellement pas de déployer un OEA si elle estime que le déploiement ne sera pas fructueux sur le plan technique, ce qui tend à indiquer un taux de réussite plus faible.
192 SCRS, « RE: [NEW RFI] NSICOP lawful access report – request for further details & clarification », 3 février 2025; GRC, « RE: [NEW RFI] NSICOP lawful access report – verification request », 4 février 2025; et RCMP, « RE: Heads up on incoming time-sensitive consultation request / fact-check », 6 février 2025.

Difficultés liées à la protection des techniques d'enquête

87. La GRC déclare faire face à d'autres grandes difficultés qui rendent de plus en plus difficile l'utilisation d'OEA par les enquêteurs. Comme l'indique le chapitre 2, lors d'une poursuite, la Couronne a l'obligation de communiquer tous les renseignements pertinents et substantiels, qui ne sont pas confidentiels, à la défense afin que les accusés puissent présenter une défense pleine et entière aux accusations portées contre eux[193]. La *Loi sur la preuve au Canada* permet au gouvernement, aux termes de l'article 37, de s'opposer à la divulgation de renseignements liés à une technique ou un outil sensible d'application de la loi et, au titre de l'article 38, de restreindre l'accès aux renseignements sensibles ou préjudiciables aux relations internationales ou à la défense ou à la sécurité nationale du Canada, y compris aux outils et aux techniques qu'utilisent les organismes de sécurité et de renseignement. D'après la GRC, bien que ces dispositions puissent s'appliquer facilement à certains outils et techniques d'enquête traditionnels, il est difficile de suivre ce processus complexe tout en respectant les échéances lorsqu'il est question d'OEA[194].

88. La GRC indique qu'elle souhaite compter sur le CST par l'entremise de demandes d'assistance pour le déploiement d'OEA, en raison des coûts et des ressources considérables que demande l'utilisation d'OEA[195]. ***[196]. Si un outil ou un moyen technique en particulier étaient divulgués au public devant les tribunaux, cette divulgation pourrait avoir des répercussions sur d'autres enquêtes en cours[197]. La GRC indique que, par conséquent, le CST *** de plus en plus incapables d'aider la GRC ou réticents à le faire, car ils craignent que ces outils doivent être divulgués devant les tribunaux[198]. D'après le CST, il n'est pas assez certain que la Couronne puisse protéger les capacités d'ERI classifiées dans les poursuites judiciaires : [traduction] « l'utilisation de l'une de ces capacités dans le cadre d'une assistance à la GRC, comportant une probabilité non négligeable d'être dévoilées lors d'une poursuite judiciaire, présente un risque inacceptable pour le CST, ses opérations et sa réputation, ***[199]. »

89. La GRC soutient qu'elle se trouve alors dans une position où elle [traduction] « doit choisir entre "vendre un outil" *** ou surseoir aux accusations en raison d'un manque de divulgation[200]. »

90. ***[201] ***[202].

193 *R. c. Stinchcombe*, [1991] 3 RCS 326.
194 Dans *R. c. Jordan*, la Cour suprême a établi des délais précis visant la clôture des procès criminels. Si un procès dépasse les délais établis sans raison valable, les accusations peuvent être suspendues. *R. c. Jordan*, 2016 CSC 27, [2016] 1 RCS 631.
195 GRC, « RCMP factual accuracy submission – NSICOP Lawful Access Draft Report », 20 décembre 2024.
196 ***
197 CST, comparution devant le CPSNR, 30 mai 2024.
198 ***
199 ***
200 GRC, « RCMP factual accuracy submission – NSICOP Lawful Access Draft Report », 20 décembre 2024.
201 ***
202 ***

91. D'après la GRC, des préoccupations en matière de divulgation ont aussi forcé le Service des poursuites pénales du Canada (SPPC) à suspendre des accusations, car la préparation pour présenter une demande de protection en application de l'article 37 ou 38 est si complexe que les retards qu'elle entraîne sont suffisamment longs pour porter atteinte au droit de l'accusé d'être jugé dans un délai raisonnable[203]. ***[204]. »

92. L'avocat de la défense et expert en droit sur la sécurité nationale, Anil Kapoor, a informé le Comité que les poursuites pénales ne représentaient pas toujours [traduction] « la façon la plus efficace de gérer les menaces envers la sécurité nationale » étant donné leurs coûts, la durée et le risque que « les informations que souhaitent protéger les organismes soient divulguées[205]. » Il a toutefois ajouté que « lorsque des ressources du renseignement courent un risque et que l'intérêt de l'accusé ou les impératifs constitutionnels pourraient demander une divulgation, […] il s'agit là de la nature des procédures pénales et il ne faudrait pas les craindre ou y voir quelque chose d'indésirable d'une certaine façon. Cela convient totalement[206]. » Selon M. Kapoor,

> les lois actuellement en vigueur offrent une approche appropriée et équilibrée à la protection des renseignements tout en prévenant le risque que des innocents soient déclarés coupables. Le problème est, sauf votre respect, de nature culturelle et il est inquiétant que les organismes soient trop réfractaires aux risques lorsqu'ils décident la façon de gérer une menace en particulier et, plus précisément, le recours aux poursuites pénales[207].

93. M. Kapoor avance que des organisations comme le SCRS et le CST ne comprennent pas suffisamment la mesure dans laquelle la loi peut protéger leurs informations sensibles devant les tribunaux[208]. Il convient de noter que M. Kapoor a réalisé en 2019 un projet d'amélioration des opérations classifié, à la demande du SCRS et de la GRC, qui examinait les décisions de la Cour fédérale entre 2008 et 2018 sous le régime de l'article 38 dans le cadre de poursuites relatives à la sécurité nationale[209]. L'examen a révélé que le gouvernement s'est appuyé sur l'article 38 pour protéger des renseignements sensibles de la divulgation dans plus de 85 % des affaires criminelles liées à la sécurité nationale, particulièrement les renseignements obtenus de partenaires internationaux[210]. L'examen a tiré comme conclusion que rien dans le critère ni les processus prévus à l'article 38 ne conduit inévitablement à la divulgation abusive de renseignements sensibles[211]. L'examen n'a toutefois pas présenté une semblable analyse concernant l'article 37.

---

203 GRC, « RCMP factual accuracy submission – NSICOP Lawful Access Draft Report », 20 décembre 2024.
204 ***
205 Anil K. Kapoor, comparution devant le CPSNR, 3 octobre 2024.
206 Anil K. Kapoor, comparution devant le CPSNR, 3 octobre 2024.
207 Anil K. Kapoor, comparution devant le CPSNR, 3 octobre 2024.
208 Anil K. Kapoor, comparution devant le CPSNR, 3 octobre 2024.
209 Les poursuites concernaient sept accusés et ont découlé des cinq enquêtes criminelles de la GRC sur la sécurité nationale suivantes (à la GRC, une enquête criminelle majeure porte le nom de projet) : projet Souvenir (*R. c. Nuttall*), projet Smooth (*R.c. Esseghaier et Jaser*), projet Slype (*R. c. Ader*), projet Servant (*R. c. Peshdary*) et projet Samossa (*R. c. Alizedeh et Ahmed*). Anil K. Kapoor et Dana C. Achtemichuk, *Projet d'amélioration des opérations*, 2019. Des accusés, quatre ont été déclarés coupables d'infractions de terrorisme, deux ont plaidé coupables et un a été reconnu non coupable. Craig Forcese et Kent Roach, *False Security: The radicalization of Canadian anti-terrorism*, 2015; Michael Nesbitt et Harman Nijjar, « Counting Terrorism Charges and Prosecutions in Canada Part 1: What does the data say? », A blog called Intrepid, 17 juin 2021; et SPPC, « Livre de transition – 2021 pour le procureur général du Canada », « Annexe 1 : Sommaire de cas des poursuites en matière de sécurité nationale — Poursuites en cours en matière de terrorisme », 17 février 2022.
210 Anil K. Kapoor, comparution devant le CPSNR, 3 octobre 2024.
211 Anil K. Kapoor et Dana C. Achtemichuk, *Projet d'amélioration des opérations*, 2019.

Autres difficultés liées au recours aux OEA

94. *** Contrairement aux États-Unis, le Canada ne dispose pas d'une politique claire qui établit le genre d'OEA commerciaux dont l'achat et l'utilisation par des organismes d'enquête du gouvernement peuvent être approuvés[212].

95. Les défenseurs de la vie privée, ainsi que des experts juridiques et en cybersécurité, critiquent vivement l'utilisation de l'ERI en raison de la quantité importante de renseignements personnels et privés que les personnes possèdent sur elles-mêmes et les autres sur leurs appareils numériques. Dans le contexte du cadre juridique du Canada, ils soutiennent que l'ERI brouille la distinction entre l'interception prospective de communications et l'extraction rétrospective de communications stockées, car le même outil peut être utilisé pour les deux opérations. Ils avancent que les dispositions actuelles du *Code criminel* et de la Loi sur le SCRS ne prévoient pas le niveau d'invasion de la vie privée que certaines fonctions d'ERI présentent, comme la capacité « d'accéder à toutes les données stockées d'une personne, peu importe qu'il s'agisse de données stockées sur l'appareil lui-même ou de données accessibles par l'entremise d'un service infonuagique auquel l'appareil est connecté[213]. » Ils indiquent aussi que les processus de demande de mandat complexes et alambiqués portent atteinte à la transparence et à la reddition de comptes[214]. La British Columbia Civil Liberties Association (BCCLA) a demandé que la loi prévoie des facteurs plus robustes en vue de guider l'utilisation d'OEA par les organismes de sécurité et d'application de la loi et d'assurer une transparence devant les Canadiens pour ce qui est des situations dans le cadre desquelles un tribunal pourrait accorder un tel mandat. Elle a aussi suggéré la mise en place d'une exigence faisant en sorte que les personnes qui ont été visées par une enquête employant un OEA en sont obligatoirement informées, à l'instar des interceptions prévues à la Partie VI, afin qu'elles puissent demander une réparation au tribunal pour toute irrégularité commise par l'organisme d'enquête[215].

96. Le Citizen Lab met en garde contre les risques que fait peser l'absence d'une réglementation de l'État sur les OEA en vente libre, qui permettent à l'industrie de mener des opérations sans faire l'objet d'une surveillance appropriée du public ou du gouvernement : [traduction] « L'existence de ce marché non réglementé a fourni à un nombre croissant de pays – y compris des pays hostiles au Canada ou ayant un historique de violation des droits de la personne – un accès à une technologie de surveillance hautement intrusive[216]. » Les défenseurs de la vie privée pourraient aussi supposer que les organismes de sécurité du Canada utilisent des OEA commerciaux, faisant valoir que [traduction] « la clandestinité caractéristique de l'industrie du logiciel espion et son utilisation par le gouvernement représentent un obstacle considérable à une reddition des comptes significative au Canada[217]. »

212 *** Maison-Blanche, « Executive Order on Prohibition of use by the United States Government of Commercial Spyware that Poses Risks to National Security », 27 mars 2023.

213 Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, document commandé par le CPSNR, décembre 2023.

214 Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, document commandé par le CPSNR, décembre 2023.

215 BCCLA, comparution devant le CPSNR, 1er octobre 2024.

216 Siena Anstis, Ronald J. Deibert, Camila Franco et Zoe Panday, « Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the NSICOP », 30 juin 2023.

217 Siena Anstis, Ronald J. Deibert, Camila Franco et Zoe Panday, « Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the NSICOP », 30 juin 2023.

97. Certaines démocraties aux vues similaires ont pris des mesures pour mettre à jour leurs lois et règlements afin de mieux refléter la technologie moderne et communiquer au public de façon plus transparente les capacités en matière de surveillance. En 2017, l'Allemagne a modifié son *Code de procédures criminelles* pour mieux tenir compte de l'application de la loi moderne, modifiant des dispositions autorisant l'extraction de communications chiffrées stockées sur un dispositif en ligne, l'accès des organismes d'application de la loi aux systèmes informatiques pour rassembler des données stockées, et l'utilisation de l'ERI pour activer à distance le microphone et la caméra d'un dispositif électronique comme moyen de surveillance[218]. En 2016, le Royaume-Uni a publié le document *Equipment Interference Code of Practice* (Code de pratique sur l'ingérence du matériel) destiné aux organismes d'application de la loi et de sécurité du pays pour les informer de la façon de mener l'ERI dans le respect de la loi. Le Code de pratique offre une orientation sur le besoin de prouver la nécessité et la proportionnalité des activités, met en place des règles entourant la manipulation de l'information et énonce des mesures de protection en matière de supervision, comme l'obtention d'une autorisation du secrétaire d'État et l'examen par le commissaire du Service du renseignement[219].

98. Selon le SCRS, un mandat propre aux OEA n'est pas nécessaire, car la Cour fédérale est au fait que [traduction] « les OEA entraînent un degré élevé d'intrusion et [la Cour fédérale] assure un équilibre avec les intérêts en matière de vie privée en imposant des conditions dans les mandats autorisant l'installation et l'utilisation d'OEA[220]. » D'après la GRC, les dispositions actuelles du *Code criminel* conviennent et répondent aux besoins de la GRC, mais elle accueille toute façon de simplifier l'obtention d'une autorisation judiciaire pour le déploiement d'un OEA[221]. Sécurité publique Canada souhaite analyser les OEA de façon plus approfondie[222].

218 Vivek Krishnamurthy, *L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?*, document commandé par le CPSNR, décembre 2023.

219 Home Office du Royaume-Uni, « Equipment Interference Code of Practice Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000 », janvier 2016.

220 SCRS, « CSIS Response to NSICOP RFI #4 on Lawful Access », 13 novembre 2024.

221 GRC, « RCMP Response to NSICOP's Review of the Lawful Access to Communications by Security and Intelligence Organizations (RFI #05) », 14 novembre 2024.

222 Sécurité publique Canada, « NSICOP Lawful Access RFI #3 to Public Safety », 15 novembre 2024.

Demandes d'assistance du CST

99. Pour surmonter les difficultés d'ordre technologique, le SCRS et la GRC ont la possibilité de présenter une demande officielle d'assistance du CST, ***[223] ***

Tableau 3.3 : Types de demandes d'assistance du CST[224]

TYPE DE DEMANDE D'ASSISTANCE	DESCRIPTION

***

100. Entre 2012 et 2023, le CST a donné suite à *** demandes d'assistance pour les deux organismes d'enquête : *** pour le SCRS et *** pour la GRC (voir les figures 3.2 et 3.3 ci-dessous). Le CST et la GRC expliquent les *** demandes de la GRC en moins par le risque que les techniques d'enquête fassent l'objet d'une divulgation devant les tribunaux, comme susmentionné, ou le choix de la GRC de ne pas aller de l'avant avec l'assistance du CST après avoir trouvé une autre solution[225]. Cela dit, tant le CST que la GRC ont cherché de plus en plus à trouver des façons pour le CST d'offrir un soutien à la GRC dans le « monde non classifié[226] », comme l'utilisation par la GRC *** du CST *** :

***[227]

***[228]

Figure 3.2 : Demandes d'assistance du CST par le SCRS : Tendances et statistiques[229]

***

Figure 3.3 : Demandes d'assistance du CST par la GRC : Tendances et statistiques[230]

***

Absence d'une législation régissant la capacité d'interception

101. Comme l'indique le chapitre 2, la capacité d'interception renvoie aux outils intégrés à un réseau ou un service de télécommunications qui permettent à un FSC d'intercepter des communications et d'autres données et de les fournir aux organismes d'application de la loi ou de renseignement en vertu d'un mandat. Aucune loi au Canada n'oblige les FSC de

223 CST, comparution devant le CPSNR, 28 mai 2024.
224 ***
225 CST, comparution devant le CPSNR, 28 mai 2024; CST, comparution devant le CPSNR, 30 mai 2024; et ***
226 CST, comparution devant le CPSNR, 30 mai 2024.
227 ***
228 CST, comparution devant le CPSNR, 28 mai 2024.
229 ***
230 ***

concevoir, de déployer et de maintenir leurs systèmes de télécommunications de façon à ce qu'ils soient aptes à l'interception de communications et de données connexes. Autrement dit, même si une autorisation judiciaire peut obliger un FSC à fournir des informations, elle ne peut pas l'obliger à fournir une connectivité technique aux organismes d'application de la loi et de sécurité[231]. Selon la GRC, sans cadre législatif, [traduction] « les processus et les capacités en matière d'accès légal ne sont pas normalisés et varient grandement[232]. »

Interception des communications par les organismes de sécurité

102. ***[233]. D'après la GRC, les outils et l'équipement d'accès légal ne changent pas le réseau en soi. Ils servent plutôt à obtenir des données qui sont déjà recueillies et stockées par un FSC dans le cadre de ses activités opérationnelles courantes ou accessibles au FSC en raison du type de service fourni, comme des services Internet[234].

103. Les données sont isolées afin que l'organisme demandeur ne reçoive que les données qu'il est légalement autorisé à consulter[235]. ***[236] ***

***[237] ***

104. La capacité d'interception ne fournit pas un accès exceptionnel, ou une porte dérobée, à du contenu chiffré. Dans un système apte à l'interception, la GRC ou le SCRS peut obtenir ou intercepter des communications à partir du réseau d'un FSC, mais ne peut pas nécessairement les lire, car le chiffrement rend souvent le contenu indéchiffrable. Certains experts en cybersécurité et défenseurs de la vie privée considèrent toutefois la capacité d'interception légale comme étant une porte dérobée en soi.

Capacité d'interception et portes dérobées

Des débats de fond sur la façon de répondre aux défis du chiffrement ont entre autres proposé que le gouvernement puisse obliger les entreprises à créer un accès exceptionnel à des programmes de chiffrement, ou des **portes dérobées**, pour les organismes de sécurité et de renseignement. Le Centre canadien pour la cybersécurité (CCC) définit une « porte dérobée » comme étant un « moyen non recensé qui permet, discrètement ou anonymement, d'accéder à distance à un ordinateur après avoir contourné les mécanismes d'authentification et s'être donné accès au texte en clair[238]. »

Selon le Citizen Lab, une fois qu'une porte dérobée est installée, rien ne garantit concrètement que seuls des organismes de l'État l'emprunteront. En raison de cette faille

231 GRC, visite du CPSNR sur place, 26 septembre 2024.
232 GRC, « International Comparison of Lawful Access Coordination and Funding Models », ébauche, 2023.
233 GRC, « RCMP factual accuracy submission – NSICOP Lawful Access Draft Report », 20 décembre 2024.
234 GRC, « RCMP's Response to NSICOP's Review of the lawful access to communications by security and intelligence organizations (RFI) #4 », 18 octobre 2024.
235 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
236 ***
237 ***
238 CCC, « Glossaire », sans date.

fondamentale, les systèmes d'accès exceptionnel constituent une menace inhérente pour les personnes qui dépendent des produits de communication chiffrés[239]. De nombreux experts de la cybersécurité partagent ce même avis[240].

Le CST a également soulevé des préoccupations concernant les portes dérobées auprès du Comité. Bien qu'il ait indiqué que [traduction] « il existe des moyens de créer des solutions techniques qui sont considérées sécuritaires actuellement[241] », il a précisé qu'une loi obligeant les FSC ou les fournisseurs de logiciels à mettre en place des portes dérobées, qui pourraient compromettre la cybersécurité plus globalement, serait pour lui une source de préoccupation[242].

D'après la GRC, [traduction] les portes dérobées « créent des vulnérabilités et peuvent affaiblir la sécurité générale d'un réseau; elles suscitent des préoccupations valables sur le plan de la sécurité, car les criminels ou d'autres acteurs hostiles peuvent exploiter ces vulnérabilités. Étant donné la nécessité de protéger les informations sensibles et de maintenir le droit des personnes à la vie privée, la GRC ne préconise pas la création de "portes dérobées" sur les réseaux des FSC. Au contraire, il serait plus sécuritaire et avantageux pour les organismes de sécurité et de renseignement de pouvoir exploiter les informations auxquelles les FSC ont déjà accès[243]. »

Certains experts en cybersécurité et défenseurs de la vie privée considèrent toutefois la capacité d'interception légale comme étant une porte dérobée, indiquant que [traduction] « il n'existe aucune porte dérobée seulement accessible par les "gentils"[244]. » D'autres avancent de même que, quoiqu'il soit possible d'affirmer que [traduction] « la technologie de la surveillance peut être développée de façon sécuritaire et sans risque de pénétration par les forces hostiles, les résultats antérieurs ne présagent rien de bon[245]. »

Ni le SCRS ni la GRC ne voit la capacité d'interception comme représentant une porte dérobée, car elle ne compromet pas les plateformes ou les logiciels de chiffrement. Ils considèrent plutôt la pratique autorisée judiciairement du recours à des outils intégrés au système d'un FSC, neutres sur le plan du chiffrement, comme s'ils utilisaient la « porte avant ».

239 Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
240 Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter et Daniel J. Weitzner, « Keys under doormats: Mandating insecurity by requiring government access to all data and communications », Massachusetts Institute of Technology Press, 6 juillet 2015; et, Susan Landau, « CALEA Was a National Security Disaster Waiting to Happen », Lawfare, 13 novembre 2024.
241 CST, « CSE Comments on NSICOP's Draft Lawful Access Report », 20 décembre 2024.
242 CST, comparution devant le CPSNR, 30 mai 2024.
243 GRC, « RCMP factual accuracy submission – NSICOP Lawful Access Draft Report », 20 décembre 2024.
244 Lawfare, citant Electronic Frontier Foundation et TechCrunch, « How Telegram Turbocharges Organized Crime », 11 octobre 2024.
245 Susan Landau, « CALEA Was a National Security Disaster Waiting to Happen », Lawfare, 13 novembre 2024.

105. En l'absence d'une législation régissant la capacité d'interception, le SCRS et la GRC dépendent de la coopération *** des FSC pour concevoir et entretenir une capacité d'interception. Des fonds sont nécessaires pour la conception et la mise en œuvre de solutions d'interception, ***[246]. Le SCRS et la GRC payent la majorité de ces coûts – ce qui avantage également les services de police municipaux et provinciaux – sans être officiellement tenus de le faire[247]. En 2022, le SCRS et la GRC ont dépensé ensemble *** $ dans la conception et l'entretien et *** $ au total en frais d'exploitation facturés par les FSC aux organismes de sécurité nationale et d'application de la loi au Canada[248].

106. Selon le SCRS et la GRC, seulement *** % des réseaux de FSC au Canada disposent d'une solution technique permettant une interception autorisée judiciairement de communications et de données connexes, et sont donc considérés comme étant aptes à l'interception, comme le montre le tableau 3.4. Le tableau ne tient toutefois pas compte des différences dans la taille des réseaux (c'est-à-dire que tous les réseaux ne sont pas égaux sur le plan de la part du marché et des usagers). Selon le Conseil de la radiodiffusion et des télécommunications canadiennes, les cinq plus grands FSC du Canada comptent pour plus de 87 % de la part des recettes[249]. ***

Tableau 3.4 : Résumé des capacités d'interception légale[250]

			NOMBRE DE RÉSEAUX EXPLOITÉS INDIVIDUELLEMENT (SERVICES)		
Catégorie de service	Nombre de FSC	Nombre total de réseaux	Apte à l'interception légale	Partiellement apte ou sous-développé	Lacune dans l'interception légale
***					

246 ***
247 GRC, comparution devant le CPSNR, 30 mai 2024.
248 SCRS et GRC, « Lawful Access Requests and Funding », sans date.
249 Conseil de la radiodiffusion et des télécommunications canadiennes, *Faits saillants annuels du secteur des télécommunications*, février 2024.
250 ***

Répercussions de l'absence d'un cadre juridique régissant la capacité d'interception

107. Selon le SCRS et la GRC, l'absence d'une législation régissant la capacité d'interception et un cadre juridique désuet entraînent des conséquences sur le plan opérationnel, financier et stratégique. En premier lieu, il n'existe aucune autorité officielle et centrale pour établir des normes ou des priorités. Par conséquent, il incombe aux FSC de filtrer de multiples demandes du SCRS, de la GRC et de services de police municipaux ou provinciaux et d'en déterminer l'ordre de priorité[251]. En l'absence de normes entourant la technologie liée à l'accès légal, les FSC choisissent la technologie qu'ils estiment être appropriée, obligeant le SCRS et la GRC à adapter chaque solution d'interception légale à l'infrastructure de chaque FSC, qui ne se transfère pas facilement d'un FSC à l'autre[252].

108. L'absence d'un cadre officiel visant à réglementer les mises à jour techniques laisse au gouvernement une mince marge de manœuvre pour contrôler les coûts. ***[253] ***[254]

109. En deuxième lieu, il n'existe aucun cadre d'indemnisation établissant qui est responsable d'assumer les coûts associés à la conception et à l'entretien de la capacité d'interception. La GRC, le SCRS et des représentants de FSC mentionnent tous des approches non uniformes au sein de la communauté de la police et du renseignement en ce qui a trait à l'indemnisation des FSC pour leurs activités et investissements entourant la capacité d'interception. Certains indemnisent les FSC pour leur coopération, tandis que ce n'est pas le cas pour d'autres, soit parce qu'ils n'ont pas les ressources ou estiment que les FSC sont tenus de soutenir la sécurité publique et la sécurité nationale ou que ces coûts, tout comme les coûts liés à la conformité de façon plus générale, devraient être vus comme étant des coûts d'entreprise[255].

110. L'une des principales préoccupations des FSC est l'absence d'un cadre d'indemnisation officiel pour réglementer le coût des solutions d'interception et le coût du traitement des demandes des enquêteurs. Un FSC a souligné que les ententes en place actuellement sont des contrats qui [traduction] « peuvent grandement varier selon les conditions de travail entre les parties concernées. Par exemple, la décision prise unilatéralement par plusieurs organismes d'application de la loi au fil des ans d'arrêter d'indemniser les FSC pour l'assistance technique, y compris les interceptions légales […] a exercé une pression financière sur les FSC et a rompu l'accord tacite que [les FSC seraient] en mesure de recouvrer les coûts liés au fonctionnement d'une nouvelle capacité [qu'ils avaient] accepté de concevoir[256]. » ***[257].

251 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
252 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
253 SCRS et GRC, comparution devant le CPSNR, 13 juin 2024.
254 SCRS, « CSIS Examples », courriel, 10 mai 2017.
255 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
256 La Cour suprême du Canada, dans sa décision de 2008 dans l'affaire *R. c. Telus*, a déterminé que les FSC ne peuvent pas facturer les services de police pour la communication de données au titre d'une ordonnance de la cour. FSC canadien, comparution devant le CPSNR, 11 juin 2024.
257 ***

111. D'après la GRC, [traduction] « pour suivre le rythme des partenaires de l'étranger, le Canada doit se doter d'un cadre d'accès légal solide et durable qui mette en place des mesures législatives, précise les responsabilités financières, simplifie l'engagement et normalise les opérations[258]. » Selon le SCRS, l'absence d'une législation régissant la capacité d'interception représente « la grande différence entre les services canadiens et leurs équivalents du Groupe des cinq : ceux-ci connaissent davantage de succès, puisque la législation sur l'accès légale [sic] leur permet de collaborer en ce sens avec les FSC[259]. » La GRC déclare que l'absence d'une législation régissant la capacité d'interception au Canada est considérée comme un obstacle ***.

112. ***[260].

113. Par exemple, ***, le FBI a envoyé des renseignements à la GRC concernant un Canadien suscitant un intérêt qui aurait été un partisan de longue date de l'État islamique[261], accumulant des armes et des matériaux de fabrication d'explosifs et planifiant d'enlever un ancien soldat canadien pour engager le gouvernement dans des négociations en cas de prise d'otages pour le compte de l'État islamique[262]. ***[263] *** Puisque les discussions sur la légalité et la faisabilité de l'ordonnance d'assistance prenaient plus de temps que prévu, les enquêteurs de la GRC ont décidé de ne pas déployer d'OEA et ont plutôt noué directement le dialogue avec l'individu, étant donné les préoccupations pour la sécurité publique[264]. Contrairement au Royaume-Uni[265] ou à l'Australie[266], les FSC au Canada ne sont pas tenus par la loi d'aider le SCRS et la GRC avec l'ERI[267].

258 GRC, « International Comparison of Lawful Access Coordination and Funding Models », ébauche, 2023.
259 SCRS et GRC, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.
260 SCRS, « CSIS Response to RFI #3: NSICOP Lawful Access Review », 17 octobre 2024.
261 L'État islamique est inscrit à la liste des entités terroristes en vertu du *Code criminel*. Sécurité publique Canada, « Entités inscrites actuellement », page Web, juin 2021.
262 GRC, « SPROS ***-570 Operational Plan Approval Request », demande d'approbation d'un plan opérationnel pour le projet ***, ***.
263 ***
264 GRC, exposé devant le Secrétariat du CPSNR, 27 novembre 2024.
265 *Investigatory Powers Act*, article 253, «Technical capability notices», 2016; Home Office du Royaume-Uni, « Explanatory Memorandum to The Investigatory Powers (Technical Capability) Regulations 2018 », 2017; Home Office du Royaume-Uni, *Equipment interference code of practice*, 2018; et Secrétaire d'État du Royaume-Uni, *The Investigatory Powers (Technical Capability) Regulations 2018*, 2018.
266 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, communément appelée TOLA, « Part 15—Industry assistance »; Ministère australien des Affaires intérieures, « The Assistance and Access Act: what does the industry assistance framework mean for domestic and international companies? », sans date, consulté en mai 2024; ministère australien des Affaires intérieures, « Scenarios – industry assistance to law enforcement and national security agencies », sans date, consulté en mai 2024; Parlement du Commonwealth de l'Australie, mémoire explicatif révisé de la TOLA, 2018; et Stilgherrian, *The Encryption Debate in Australia: 2021 Update*, Carnegie Endowment for International Peace, 2021.
267 SCRS, « Éviter de se retrouver dans le noir (de perdre l'accès aux informations) : Protection des pouvoirs de collecte dans un monde numérique », 18 avril 2024.

114. Les FSC indiquent également que leur entreprise doit trouver un équilibre entre la perception du public et le risque à la réputation, et la responsabilité organisationnelle entourant l'approche volontaire de répondre aux demandes d'accès légal. Selon eux, une législation obligeant la coopération atténuerait ces risques[268]. Sécurité publique Canada résume les conséquences opérationnelles, financières et stratégiques de l'approche volontaire de l'accès légal dans le tableau 3.5 ci-dessous.

Tableau 3.5 : Conséquences opérationnelles, financières et stratégiques de l'approche volontaire de l'accès légal[269]

SITUATION ACTUELLE	CONSÉQUENCE
Aucune exigence liée à la capacité d'interception pour les nouvelles technologies, et lorsque les normes du solliciteur général s'appliquent, les FSC pourraient quand même refuser de coopérer.	• Lacunes importantes de la couverture d'interception, surtout pour les nouvelles technologies. • Le Canada traîne de la patte derrière ses pairs.
Le SCRS et la GRC payent la majorité des coûts de conception et d'entretien et doivent négocier individuellement les coûts avec les FSC.	• Contrôle limité du gouvernement sur les coûts. • Aucune normalisation des coûts entre les FSC ou les organismes, tant sur le montant à verser que le moment où le verser.
Le SCRS et la GRC financent les solutions d'interception pour tous les organismes d'application de la loi, sans mandat pour ce modèle.	• Le gouvernement fédéral supporte la majorité des coûts, y compris pour les interceptions des organismes locaux et provinciaux d'application de la loi.

***

Pallier le manque de législation régissant la capacité d'interception

115. Le SCRS et la GRC affirment avoir pallié les difficultés posées par l'approche volontaire de la capacité d'interception en assurant une étroite coordination de leurs activités. Le SCRS et la GRC concluent des protocoles d'entente annuels à l'appui de la conception, du soutien et de l'entretien de la capacité d'interception et partagent les coûts associés aux ententes de services avec les FSC[270]. ***[271] ***[272] ***[273]

268 FSC canadien, comparution devant le CPSNR, 11 juin 2024.
269 Adapté de Sécurité publique Canada, comparution devant le CPSNR, présentation, 11 avril 2024.
270 SCRS et GRC, « Lawful Access Requests and Funding », sans date.
271 ***
272 SCRS, comparution devant le CPSNR, 18 avril 2024; et Sécurité publique Canada, comparution devant le CPSNR, 11 avril 2024.
273 SCRS et GRC, comparution devant le CPSNR, 18 avril 2024.

116. En 2023, le SCRS et la GRC ont créé officieusement le Centre national pour l'accès légal (CNAL) comme point de coordination central en matière d'accès légal au Canada pour tous les organismes d'application de la loi et de renseignement nationaux[274]. En novembre 2024, le gouvernement n'avait pas encore officialisé le CNAL, mais le Centre serait chargé [traduction] « d'établir des normes et des processus nationaux en matière d'accès légal, de gérer la collecte de données en matière d'accès légal et la technologie de l'infrastructure du réseau communes, et d'assurer la coordination avec les fournisseurs de services, tous les niveaux de l'application de la loi et les partenaires fédéraux au nom des organismes canadiens chargés de l'application de la loi et de la sécurité nationale[275]. »

117. En 2023, le SCRS et la GRC ont aussi créé le Comité consultatif pour l'accès légal (LAAC), qui a tenu sa première réunion en novembre 2023. Le comité est coprésidé par la GRC et le directeur de la sécurité d'un grand FSC, et regroupe sept grands FSC. Selon le SCRS et la GRC :

> [traduction] La création du LAAC officialise l'intention et l'engagement du gouvernement autant que de l'industrie privée de collaborer à l'élaboration de solutions à long terme en vue de résoudre les difficultés de longue date liées à l'accès légal. […] Le LAAC se penchera sur les difficultés et examinera des solutions liées à l'accès légal, comme l'élaboration d'un cadre de gouvernance de l'accès légal canadien, la création d'un modèle d'indemnisation pour les services des FSC, la conception et l'intégration de nouvelles solutions et capacités techniques d'accès légal, et la mise en œuvre d'une stratégie nationale visant à assurer une compréhension commune de l'accès légal par tous les membres de la communauté de l'accès légal au Canada[276].

118. Dans son cadre de gouvernance, le LAAC établit plusieurs principes directeurs, dont le premier inscrit la vie privée comme l'un des piliers fondamentaux de l'accès légal, ainsi qu'un engagement à veiller à ce que les pratiques en matière d'accès légal [traduction] « respectent l'équilibre entre la sécurité et la sûreté des Canadiens et la vie privée et la protection des renseignements personnels[277]. » Les principes comprennent aussi la normalisation par défaut, au titre de laquelle les organismes de sécurité et les FSC chercheront à normaliser leurs solutions et processus techniques. Un autre principe clé comprend un engagement envers un modèle d'indemnisation juste qui n'entraîne pas de coûts :

> La communauté de l'accès légal reconnaît que les FSC sont des entreprises privées ou semi-privées qui méritent de recevoir une indemnisation juste pour les efforts nécessaires à la conception, à l'entretien et au fonctionnement des capacités qui ne font pas partie de leurs processus opérationnels habituels. Les FSC chercheront à réaliser des opérations d'accès légal sans engager de coûts (c'est-à-dire qu'ils ne tirent pas de gains financiers ni ne subissent de pertes financières lorsqu'ils offrent un soutien judiciairement autorisé aux organismes demandeurs). Ces coûts comprennent la conception de solutions techniques, l'entretien et l'exploitation de ces solutions, et d'autres services connexes[278].

Selon le FSC coprésident, le niveau de coopération entre les organismes de sécurité et les

274 GRC, « National Lawful Access Centre – Unclassified », sans date.
275 GRC, « National Lawful Access Centre – Unclassified », sans date.
276 SCRS et GRC, « Creation of and Invitation to Participate in the Lawful Access Advisory Committee », 30 août 2023.
277 SCRS et GRC, « Creation of and Invitation to Participate in the Lawful Access Advisory Committee », 30 août 2023.
278 SCRS et GRC, « Creation of and Invitation to Participate in the Lawful Access Advisory Committee », 30 août 2023.

FSC dans l'année suivant la création du LAAC n'a jamais été aussi élevé qu'au cours de la dernière décennie en entier[279].

119. Entre 2012 et 2024, les défenseurs de la vie privée ont critiqué sans cesse les propositions et les consultations de projets de loi en vue de la création d'une législation régissant la capacité d'interception sous prétexte que le gouvernement n'avait pas présenté assez de preuve montrant le problème ou n'était pas parvenu à estimer avec précision les coûts prévus potentiellement très élevés (le chapitre 4 aborde le sujet plus en détail). Plus récemment, M. Geist a aussi averti de ne pas se concentrer trop attentivement sur l'infrastructure de télécommunications traditionnelle dans l'étude de la modernisation de la législation régissant l'accès légal. Il attire l'attention sur le rôle plus faible des FSC dans la fourniture du contenu des communications en raison de la prévalence grandissante de services de messagerie par contournement chiffrés de bout en bout sur Internet : [traduction] « La politique entourant l'accès légal est depuis longtemps centrée sur le rôle des intermédiaires de communication comme les fournisseurs de services Internet et sans fil. Toutefois, la réalité d'aujourd'hui est telle que les communications ne sont plus facilitées principalement exclusivement par leur infrastructure[280]. »

120. D'après la GRC, il faut adopter des dispositions législatives prévoyant notamment des exigences pour les FSC canadiens, y compris [traduction] « les applications par contournement, les fournisseurs de services par satellite, les revendeurs de services de communication et certains fabricants de véhicules dont les produits comprennent des moyens de communication intégrés[281]. »

Nature transfrontalière des données numériques : répercussions et activités d'atténuation

121. Le SCRS et la GRC affirment que la nature mondiale d'Internet entraîne d'importants défis sur le plan des compétences et retards. Alors que les plateformes sur Internet et les services de communication en temps réel ont [traduction] « joué un grand rôle dans la facilitation de services de communication sur réseau », ils sont « rarement établis au Canada, utilisent différents niveaux de chiffrement, peuvent mettre en place des normes divergentes pour la communication aux organismes d'application de la loi et publient fréquemment des rapports exhaustifs sur la transparence[282]. »

279 FSC canadien, comparution devant le CPSNR, 11 juin 2024.

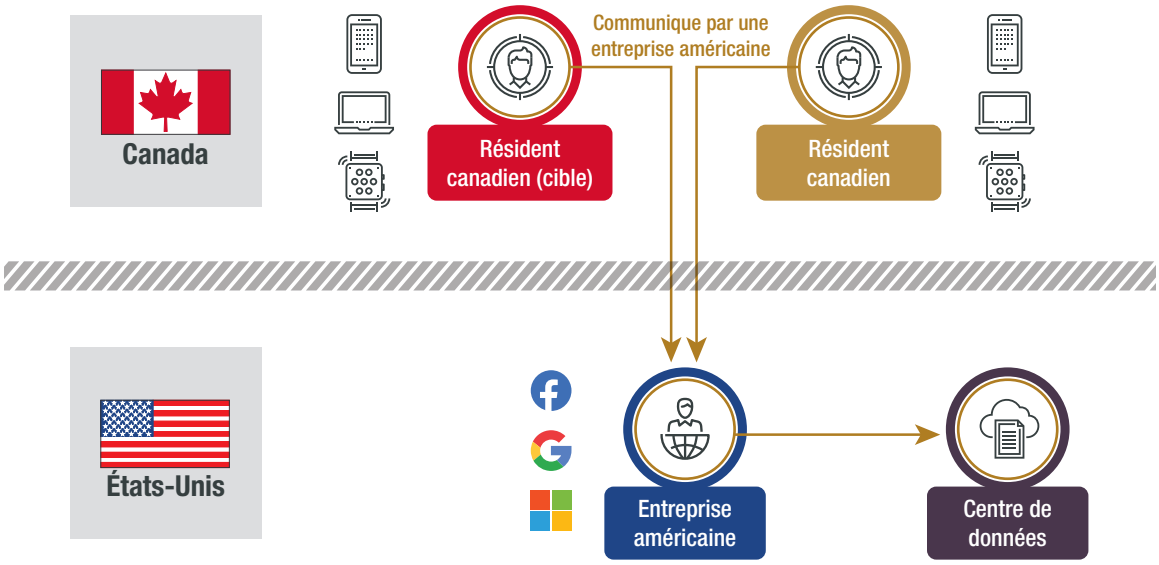
280 Michael Geist, *Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes Internet*, document commandé par le CPSNR, mai 2024.

281 GRC, « RCMP's Response to NSICOP's Review of the lawful access to communications by security and intelligence organizations (RFI) #4 », 18 octobre 2024.

282 Michael Geist, *Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes Internet*, document commandé par le CPSNR, mai 2024.

122. Bon nombre des services de communications les plus populaires utilisés par les Canadiens sont établis aux États-Unis (comme Google, Facebook et Apple), comme le montre la figure 3.5[283]. Au titre de la *Stored Communications Act* des États-Unis, il est illégal pour les entreprises américaines de divulguer le contenu de communications à des gouvernements étrangers à moins d'une ordonnance signifiée par les tribunaux américains[284].

Figure 3.5 : Bon nombre des services de messagerie les plus populaires utilisés par les Canadiens sont établis aux États-Unis[285]



123. Si elle doit obtenir des informations numériques de la part d'une entreprise établie à l'extérieur du Canada, la GRC peut en faire la demande par l'entremise d'un traité d'entraide juridique (TEJ), lorsqu'un tel traité a été conclu[286]. Par exemple, si la GRC requiert des informations d'une entreprise comme Facebook ou Apple, elle envoie une demande au ministère de la Justice du Canada, qui l'envoie au département de la Justice américain. Lorsque le département de la Justice américain accepte une demande, un procureur adjoint des États-Unis présente la demande à un juge américain pour qu'il délivre un mandat en vue de l'obtention des informations. Le Federal Bureau of Investigation (FBI) peut ensuite exécuter le mandat délivré par le juge américain[287]. Lorsque l'entreprise fournit les informations au FBI, elles sont envoyées à la GRC par l'entremise du département de la Justice et du ministère de la Justice. Même si la procédure judiciaire se déroule sans heurts, le contenu demandé par un enquêteur pourrait être supprimé avant la réception de la demande juridique si l'entreprise n'applique pas une politique de rétention des données[288].

283 Sécurité publique Canada, « U.S. CLOUD Act: DMNS Presentation », 22 février 2019.
284 SCRS, « The U.S. *CLOUD Act* and Opportunities for CSIS: Executive Brief », sans date.
285 Sécurité publique Canada, « U.S. CLOUD Act: DMNS Presentation », 22 février 2019.
286 Le Canada adhère à plus de trente TEJ bilatéraux. Robert J. Currie et Joseph Rikhof, *International & Transnational Criminal Law*, 2020.
287 Département de la Justice, « Justice Response for Factual Accuracy », 20 décembre 2024.
288 Michael Geist, *Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes Internet*, document commandé par le CPSNR, mai 2024.

124. Selon la GRC, le processus lié au TEJ peut prendre de trois à six mois, et ce laps de temps peut nuire aux enquêtes[289]. En 2016, le département américain de la Justice a décrit le processus lié au TEJ comme étant [traduction] « un mécanisme important, mais qui exige souvent une main-d'œuvre abondante pour la facilitation de la coopération avec les organismes d'application de la loi, [et il] doit faire face aux difficultés qu'entraîne la hausse considérable de la quantité et de la complexité des demandes d'aide présentées aux États-Unis à l'ère d'Internet » alors que de nombreux FSC mondiaux de premier plan s'y sont établis[290]. *** le processus lié au TEJ n'a pas été conçu pour traiter [traduction] « une très grande quantité de demandes d'éléments de preuve électroniques à vive allure[291]. »

125. Le SCRS ne peut pas se prévaloir des TEJ. ***[292] ***[293] ***[294]

126. La GRC et le SCRS estiment tous deux qu'il existe une solution possible aux défis sur le plan des compétences se rapportant aux États-Unis, soit en tirant parti de la *Clarifying Lawful Overseas Use of Data Act* des États-Unis, ou la CLOUD Act. Adoptée en 2018, la CLOUD Act cherche à accélérer l'accès aux informations électroniques détenues par des FSC mondiaux établis aux États-Unis[295]. Le Canada et les États-Unis négocient actuellement un accord sur l'accès aux données afin de permettre à leurs organismes d'application de la loi et de sécurité respectifs de demander des données, y compris le contenu de communications, auprès des fournisseurs de services de chaque pays (le point est abordé plus en détail au chapitre 4).

127. Apple, Facebook, Google et Microsoft soutiennent publiquement l'approche de la CLOUD Act relativement à l'échange transfrontalier de données, soulignant que [traduction] « elle permettrait aux organismes d'application de la loi de mener des enquêtes sur le terrorisme et la criminalité transfrontalière sans créer de conflits juridiques internationaux[296]. » ***[297] ***[298]

128. Certains FSC du Canada ont soulevé des préoccupations concernant la façon dont ils pourront répondre aux éventuelles demandes des États-Unis si et quand un accord bilatéral sur l'accès des données est conclu, surtout compte tenu de l'absence d'un cadre juridique régissant la capacité d'interception[299].

289 GRC, comparution devant le CPSNR, 18 avril 2024.
290 Procureur général adjoint des États-Unis, *Letter to the Honourable Joseph R. Biden, President of the United States Senate*, 15 juillet 2016.
291 ***
292 SCRS, « 2022 11 25 NSICOP Meeting Write Up », novembre 2022.
293 ***
294 ***
295 Département de la Justice des États-Unis, « Promoting Public Safety, Privacy, and the Rule of Law Around World: The Purpose and Impact of the CLOUD Act White Paper », avril 2019.
296 Apple, Facebook, Google, Microsoft et Oath, « Letter to U.S. Senators Orrin Hatch, Christopher Coons, Lindsey Graham, and Sheldon Whitehouse », 6 février 2018.
297 ***
298 ***
299 Représentant d'un FSC, comparution devant le CPSNR, 3 octobre 2024.

Chapitre 4 : Réponse du gouvernement

129. Le chapitre précédent décrit les interventions opérationnelles des organismes de sécurité et de renseignement en réaction aux défis liés à l'accès légal, ce que le Comité perçoit comme étant des mesures « ascendantes » visant à atténuer lesdits défis selon les limites du cadre d'accès légal en vigueur au Canada. Or, le présent chapitre se penche sur les mesures « descendantes » suivant lesquelles le gouvernement a tenté de moderniser ledit cadre entre 2012 et la fin de 2024. Pendant cette période, le gouvernement a voulu résoudre les difficultés de l'accès légal par l'entremise de plusieurs initiatives stratégiques intersectorielles, notamment en promouvant l'adoption de mesures législatives, en menant des consultations publiques, en orchestrant des mesures de financement et en poursuivant la coopération internationale. Le Comité a choisi de présenter la réponse du gouvernement de façon chronologique, en fonction des sessions parlementaires.

Responsables des politiques et gouvernance

130. Le ministre de la Sécurité publique et le ministre de la Justice sont responsables envers le Parlement pour ce qui a trait à l'accès légal. En outre, ils sont conseillés par le ministère de la Sécurité publique et de la Protection civile et le ministère de la Justice, et les principaux organes opérationnels dont ils sont responsables sont le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC). Pendant la période visée par le présent examen, une succession de comités du Cabinet auraient pu servir de forums propices aux discussions sur la politique d'accès légal[300]. Selon le ministre de la Sécurité publique, le Comité du Cabinet chargé des affaires internationales et de la sécurité publique est l'instance la plus probable où se tiendraient des discussions sur la politique en matière d'accès légal, comparativement au nouveau Conseil de la sécurité nationale, qui s'est réuni une première fois en octobre 2023.

131. Les délibérations du Cabinet sur la politique d'accès légal bénéficient de l'appui du Comité des sous-ministres sur la sécurité nationale (CSMSN). Le mandat du CSMSN est d'analyser les enjeux liés à la sécurité, à la défense et à la politique étrangère dans le but de formuler des conseils cohérents et intégrés à l'intention du premier ministre et des comités du Cabinet[301]. Généralement coprésidé par le conseiller à la sécurité nationale et au renseignement et le sous-ministre de la Sécurité publique, ce comité réunit les

300 Il s'agit entre autres du Comité du Cabinet chargé des affaires étrangères et de la sécurité (de février 2006 à novembre 2015), du Comité du Cabinet chargé de la sécurité nationale (de mai 2011 à juillet 2013), du Comité du Cabinet chargé des affaires du Canada dans le monde (de novembre 2015 à septembre 2023), renommé le Comité du Cabinet chargé des affaires internationales et de la sécurité publique en septembre 2023, et du Conseil de la sécurité nationale (à partir d'octobre 2023).

301 CSMSN, « Mandat », sans date.

administrateurs généraux d'Affaires mondiales Canada (AMC), du Centre de la sécurité des télécommunications (CST), de la GRC, d'Innovation, Sciences et Développement économique Canada (ISDE), du ministère de la Justice et du SCRS[302].

132. Plusieurs enjeux distincts mais interreliés en matière d'accès légal ont été étudiés par le gouvernement pendant la période visée par le présent examen. Parmi ces enjeux, mentionnons :

- cadre juridique régissant la capacité d'interception des fournisseurs de services de communication (FSC) canadiens;
- élaboration d'une loi régissant l'accès aux renseignements de base sur les abonnés (RBA), comme suite à la décision rendue par la Cour suprême dans l'affaire *R. c. Spencer*;
- élaboration d'une politique sur le chiffrement qui indique, notamment, s'il convient d'exiger que les FSC et les autres plateformes de communication déchiffrent les communications sur demande des enquêteurs;
- nécessité de contraindre légalement les FSC à conserver les métadonnées pour une durée déterminée;
- négociation de traités autorisant l'accès à l'information détenue par des FSC situés à l'étranger grâce à la promotion de la coopération multilatérale, mais aussi de la coopération entre le Canada et les États-Unis.

Réponse du gouvernement aux défis de l'accès légal

Démarches antérieures

133. La réponse du gouvernement aux questions liées à la politique d'accès légal précède la période visée par l'examen. En 1998, le gouvernement a publié sa politique en matière de cryptographie aux fins du commerce électronique, laquelle reconnaissait les défis posés pour les organismes d'application de la loi, mais favorisait les produits de chiffrement puissants dans la mesure où ils sont des outils essentiels sur lesquels reposent la prospérité économique et l'économie numérique[303].

134. En 1999, le gouvernement a mis sur pied l'Initiative d'accès légal dont l'objectif était de [traduction] « mettre en place un cadre stratégique » conçu pour aider les organismes d'application de la loi (la GRC et les services de police autres que fédéraux) et les autres organismes de sécurité (le SCRS et le CST) à [traduction] « garantir l'accès légal à l'information et aux communications[304] ». Dirigée par Sécurité publique Canada, cette initiative regroupait le SCRS, le ministère de la Justice, ISDE, le CST, le Service des

302 Membres : Affaires mondiales Canada (AMC), Agence canadienne d'inspection des aliments (ACIA), Agence de la santé publique du Canada (ASPC), Agence des services frontaliers du Canada (ASFC), Bureau du Conseil privé (BCP) – conseiller à la sécurité nationale et au renseignement (CSNR) auprès du premier ministre (coprésident), Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), CST, Forces armées canadiennes (FAC), GRC, Immigration, Réfugiés et Citoyenneté Canada (IRCC), Innovation, Sciences et Développement économique Canada (ISDE), ministère de la Défense nationale, ministère des Finances, ministère de la Justice, SCRS, Sécurité publique Canada (coprésident), et Transports Canada. BCP, « Governance Structure – National Security », sans date.

303 Industrie Canada, *Politique cadre en matière de cryptographie aux fins du commerce électronique : Pour une économie et une société de l'information au Canada*, février 1998.

304 Solliciteur général du Canada, ministre de la Défense nationale et ministre de la Justice, « Maintenir l'accès légal à l'information et aux communications requises pour assurer la sécurité du public », mémoire au Cabinet, 17 février 1999.

poursuites pénales du Canada (SPPC) et la GRC. Le gouvernement du Canada a financé l'initiative pendant les cinq premières années à hauteur de *** $ par année et a fourni un financement permanent de *** $ à partir de 2005 jusqu'à aujourd'hui. L'initiative donne au SCRS et à la GRC les fonds pour les solutions d'interception dans les installations des FSC, le traitement et l'analyse, et *** techniques[305].

135. Les efforts que le gouvernement a consentis à la modernisation des lois s'appliquant à l'accès légal à l'ère du numérique ont commencé à être sérieux après la signature, en novembre 2001, de la *Convention de Budapest sur la cybercriminalité* du Conseil de l'Europe, un accord multilatéral qui engage le gouvernement à inscrire, dans le *Code criminel*, de nouveaux pouvoirs relatifs aux éléments de preuve électroniques, particulièrement pour ce qui a trait aux ordonnances de communication spécialisées[306]. Entre 2001 et 2004, le gouvernement a tenu plusieurs consultations publiques portant sur la question de l'accès légal dans le but d'orienter les propositions législatives. Puis, de 2005 à 2012, le gouvernement a déposé sept projets de loi visant à actualiser le droit canadien en matière d'accès légal. Or, tous ces projets de loi sont morts au Feuilleton à la suite de la dissolution ou de la prorogation du Parlement. Aucun n'est donc entré en vigueur. Voir l'Annexe E.

136. Les projets de loi se sont attiré les critiques de défenseurs de la vie privée, d'experts en cybersécurité et de FSC[307], qui ont fait valoir que le gouvernement n'avait pas suffisamment prouvé l'existence du problème, n'avait pas expliqué pourquoi les pouvoirs existants étaient insuffisants et ne pouvait pas indiquer combien coûterait l'initiative[308]. De fait, des experts en cybersécurité et des défenseurs de la vie privée ont manifesté leur inquiétude à l'égard de toute tentative d'imposer, au titre de la loi, l'introduction de vulnérabilités dans le chiffrement suivant l'insertion de portes dérobées exploitables par les organismes d'application de la loi et de sécurité, en partie pour la simple raison que ces vulnérabilités pourraient très bien être exploitées par des acteurs malveillants[309].

---

305 Depuis 2005, l'Initiative d'accès légal a fourni au SCRS *** $ annuellement, y compris *** équivalents temps plein (ETP), et *** $ annuellement à la GRC, y compris *** ETP, totalisant (pour les deux organisations) *** $ annuellement, y compris *** ETP. SCRS, « CSIS Funding Letter », du directeur adjoint de la Technologie du SCRS au sous-ministre délégué de la Sécurité publique, 17 avril 2013; SCRS, feuille de calcul d'établissement des coûts du SCRS créée pour le CPSNR pour donner suite à la demande de renseignements nº 2, reçue le 13 septembre 2024; et Sécurité publique Canada, *Lawful Access Initiative: Final Performance Measurement Report, Fiscal Years 2015-2018*, sans date.

306 La Convention de Budapest harmonise les infractions en matière de cybercriminalité et les ordonnances de communication en vue de l'obtention d'éléments de preuve numériques et sert de traité d'entraide juridique pour les 76 pays qui l'ont ratifiée en date de septembre 2024. Conseil de l'Europe, *Convention sur la cybercriminalité*, 23 novembre 2001; et Conseil de l'Europe, « Tableau des signatures et ratifications du traité 185 », septembre 2024.

307 Christopher Parsons, « Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada », chapitre IX de Michael Geist (directeur de publication), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Les Presses de l'Université d'Ottawa, 2015.

308 Michael Geist, « Why The Government's Lawful Access Claims Stand on a Shaky Foundation », 12 décembre 2011; Michael Geist, « Everything You Always Wanted to Know About Lawful Access, But Were (Understandably) Afraid to Ask », 13 février 2012; Michael Geist, « How to Fix Canada's Online Surveillance Bill: A 12 Step To-Do List », 24 février 2012; Kevin McArthur et Christopher Parsons, « Understanding the Lawful Access Decryption Requirement », 18 septembre 2012; Christopher Parsons, « Lawful Access, Its Potentials, and its Lack of Necessity », 9 novembre 2011 (republié le 18 août 2022); et commissaire à la protection de la vie privée du Canada, « Lettre au ministre de la Sécurité publique », communiqué de presse, 26 octobre 2011.

309 CST, « Policy Considerations on End-to-End Encryption », sans date; Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter et Daniel J. Weitzner, « Keys under doormats: Mandating insecurity by requiring government access to all data and communications », Massachusetts Institute of Technology Press, 6 juillet 2015; Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018; et Kevin McArthur et Christopher Parsons, « Understanding the Lawful Access Decryption Requirement », 18 septembre 2012.

41e législature (de 2011 à 2015)

137. Chacune des tentatives par lesquelles le gouvernement a cherché à adopter une loi en matière d'accès légal était tirée des précédents échecs et comportait les mêmes dispositions ou des dispositions semblables[310]. En février 2012, le gouvernement a déposé le projet de loi C-30 intitulé *Loi sur la protection des enfants contre les cyberprédateurs*[311]. Le projet de loi aurait édicté la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, obligeant les FSC à disposer d'une capacité d'interception et de déchiffrement des communications chiffrées. Il aurait également inscrit, dans le *Code criminel*, des ordonnances de communication spécialisées permettant aux enquêteurs d'obtenir certaines données électroniques qui suscitent des attentes plus faibles en matière de respect de la vie privée, notamment les données de géolocalisation[312]. Or, le projet de loi a tôt fait de s'attirer les mêmes critiques que celles reçues par les projets de loi précédents. Ainsi, en février 2013, le ministre de la Justice a publiquement mis le projet de loi de côté et a indiqué que tous les projets de loi [traduction] « visant à moderniser le *Code criminel* ne proposeraient aucune des mesures contenues dans le projet de loi C-30[313] ».

138. En novembre 2013, le gouvernement a déposé le projet de loi C-13 intitulé *Loi sur la protection des Canadiens contre la cybercriminalité*, qui est entré en vigueur en mars 2015. Celui-ci conservait les parties les moins controversées du projet de loi C-30, à savoir les nouveaux ordres et ordonnances de préservation ainsi que les ordonnances de communication spécialisées[314]. L'entrée en vigueur de la *Loi sur la protection des Canadiens contre la cybercriminalité* a permis au Canada de ratifier la *Convention de Budapest sur la cybercriminalité* du Conseil de l'Europe, qui est entrée en vigueur au Canada le 1er novembre 2015[315]. Suivant l'adoption de la Loi, le gouvernement a mis en place l'initiative Les pouvoirs d'enquête au XXIe siècle (PE21S) dans le but de soutenir la mise en œuvre de ladite Loi et l'exercice des obligations du Canada au titre de la Convention de Budapest. Dirigée par le ministère de la Justice en collaboration avec le SPPC, la GRC et AMC, l'initiative avait pour objet d'informer les procureurs canadiens et les services de police étrangers au sujet des nouveaux pouvoirs prévus par la Loi, de favoriser la coopération internationale dans le cadre de la Convention de Budapest et, dans le cas de la GRC, d'élargir les capacités en matière de criminalistique numérique. Aux fins de PE21S, le gouvernement a accordé aux quatre ministères et organismes un financement à hauteur de 60,74 millions $ sur cinq ans (de 2015-2016 à 2019-2020), puis un financement permanent de 12,25 millions $ (à partir de 2020-2021)[316].

310 Il s'agit du projet de loi C-74, la *Loi sur la modernisation des techniques d'enquête* en 2005; du projet de loi C-46, la *Loi sur l'assistance au contrôle d'application des lois au 21e siècle* en 2009; et du projet de loi C-52, la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention* en 2010.

311 Titre complet : *Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois*.

312 Ces ordonnances de communication figurent dans la loi depuis l'entrée en vigueur de la *Loi sur la protection des Canadiens contre la cybercriminalité* en mars 2015.

313 Citation du ministre de la Justice dans Laura Payton, « Government killing online surveillance bill », CBC News, 11 février 2013.

314 Il s'agissait notamment d'ordonnances de communication spécialisées et de nouveaux pouvoirs au titre du *Code criminel* permettant à la police d'obliger les entités canadiennes à conserver des données informatiques jusqu'à ce que l'enquêteur détienne les motifs obligeant lesdites entités de lui fournir les données en question.

315 Conseil de l'Europe, « Tableau des signatures et ratifications du traité 185 », septembre 2024.

316 Ministère de la Justice, *Évaluation de l'Initiative sur les pouvoirs d'enquête au 21e siècle*, rapport final, mars 2020.

139. En juin 2014, la Cour suprême a rendu une décision unanime dans l'affaire *R. c. Spencer*, selon laquelle il y avait une attente raisonnable en matière de vie privée à l'égard des RBA, dès lors que ceux-ci sont liés à une adresse de protocole Internet. La décision de la Cour suprême donnait au gouvernement deux options : la police pouvait se servir des pouvoirs déjà inscrits dans le *Code criminel* ou le gouvernement pouvait présenter une nouvelle « loi qui n'a rien d'abusif » permettant à la police d'accéder aux RBA[317]. Le ministère de la Justice et ses pendants provinciaux et territoriaux ont déployé des efforts concertés visant à bien saisir l'incidence opérationnelle de l'arrêt *Spencer* et à analyser les questions relatives à la loi et à la vie privée, notamment la jurisprudence postérieure à 2014 dans la mesure où les tribunaux ont appliqué l'arrêt *Spencer* à diverses causes[318]. ***

42e législature (de 2015 à 2019)

140. En octobre 2015, les Canadiens ont élu un nouveau gouvernement. Le mois suivant, le premier ministre a chargé la ministre de la Justice ainsi que le ministre de la Sécurité publique et de la Protection civile d'adopter de nouvelles mesures législatives en matière de sécurité nationale. De septembre à décembre 2016, le gouvernement a tenu des consultations publiques concernant cette proposition de loi à partir d'un livre vert sur la sécurité nationale[319]. Ayant pour but « d'engager une discussion et un débat au sujet du cadre de sécurité nationale du Canada », le livre vert comprenait un chapitre intitulé « Capacités d'enquête dans le monde numérique », qui mettait en évidence quatre enjeux essentiels : les RBA, la capacité d'interception, la conservation des données et le chiffrement. Ce livre comptait également un chapitre intitulé « Renseignement et preuve »[320].

141. ***[321] ***[322] ***[323] ***[324] ***[325]

142. En mai 2017, Sécurité publique Canada a publié le rapport *Ce que nous avons appris* sur les consultations tenues dans le contexte du livre vert. Sécurité publique Canada avait tenu cinq assemblées publiques en personne, quatorze séances en personne avec des universitaires et des experts ainsi qu'une table ronde avec des experts de la société civile. Les ministres de la Sécurité publique et de la Protection civile et de la Justice ont codirigé plusieurs événements, y compris la table ronde à laquelle 36 experts de la société civile ont participé[326]. Les secrétaires parlementaires des deux ministres ont aussi animé des événements; notamment, le secrétaire parlementaire de la ministre de la Justice a organisé une assemblée à Yellowknife, dans les Territoires-du-Nord-Ouest[327]. Des députés ont aussi organisé dix-sept événements de mobilisation dans leur circonscription auxquels ont participé des membres du public. Sécurité publique Canada a reçu 58 933 réponses au questionnaire en ligne, 17 862 envois par courriel en plus de 79 mémoires de la part d'organisations et d'experts.

317 *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212.
318 ***
319 Sécurité publique Canada, *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*, 19 mai 2017.
320 Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale, 2016*, 2016; et gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016 : Document de contexte*, 2016.
321 ***
322 ***
323 ***
324 ***
325 ***
326 Sécurité publique Canada, « Table ronde sur le cadre de sécurité nationale Soirée des experts de la société civile – 19 octobre 2016 », résumé, 29 novembre 2016.
327 Sécurité publique Canada, « Assemblée publique sur le Cadre de sécurité nationale à Yellowknife – Le 5 décembre 2016 », résumé, 23 décembre 2016.

La partie de la consultation portant sur l'accès légal a généré environ 70 % de toutes les réponses en ligne et une contribution considérable de la part d'experts et d'organisations, ce qui témoigne d'une importante participation de la part du public et des intervenants. En outre, la grande majorité des réponses indiquaient que dans un monde numérique, l'attente en matière de vie privée est égale, voire supérieure à celle qui est suscitée dans le monde réel. La nette majorité des répondants s'opposaient à toute mesure visant à affaiblir le chiffrement, et sept répondants sur dix considéraient que les renseignements de base les concernant en tant qu'abonnés devaient avoir le même niveau de confidentialité que celui de leurs courriels ou de leur journal intime. Près de la moitié (44 %) des répondants ayant rempli le questionnaire en ligne ne reconnaissaient pas le besoin de donner de nouveaux outils aux enquêteurs, quoique 41 % des réponses soumises en ligne indiquaient que les enquêteurs devraient avoir accès à des outils modernes adaptés au monde numérique s'ils sont en mesure d'en montrer la nécessité[328].

143. L'analyse interne de Sécurité publique Canada sur la consultation de 2016 a souligné les opinions de 35 entités notables y compris de représentants de l'application de la loi et de la société civile, d'universitaires, de FSC et de commissaires fédéraux, provinciaux et territoriaux à la protection de la vie privée : [traduction] « Dans l'ensemble des thèmes, les intervenants étaient d'avis qu'on ignorait pourquoi les pouvoirs prévus par la loi n'étaient pas adaptés aux besoins des enquêteurs. De nombreux intervenants ont demandé au gouvernement de montrer clairement en quoi des changements étaient nécessaires. » Ces intervenants ont répondu aux quatre enjeux en matière d'accès légal du livre vert :

- ***Accès légal aux RBA :*** « La plupart des intervenants, issus des secteurs de la société civile, du milieu universitaire et des FSC, estimaient que les enquêteurs devraient obtenir une autorisation judiciaire pour accéder aux RBA. »
- ***Capacité d'interception des réseaux de FSC :*** « Bien qu'ils n'aient pas montré un appui envers la proposition, la plupart des intervenants des FSC ne se sont pas carrément opposés à la mise en place d'exigences relatives à la capacité d'interception » pourvu que les exigences « ne perturbent pas les opérations ou la concurrence » et que le gouvernement les indemnise.
- ***Conservation des données :*** « De nombreux intervenants de la société civile, du milieu universitaire et des FSC, ainsi que des commissaires FPT à la protection de la vie privée ont remis en question le besoin de créer des exigences relatives à la conservation des données étant donné que des pouvoirs liés à la préservation des données avaient été édictés [dans le *Code criminel*] en 2015. » « Les intervenants des FSC et de la société civile qui ne s'étaient pas opposés de façon absolue à la conservation des données ont tout de même soulevé d'importantes préoccupations concernant les répercussions possibles d'une telle mesure sur la vie privée des Canadiens et la sécurité de leurs données. »
- ***Chiffrement :*** « Des intervenants, issus des secteurs de la société civile, du milieu universitaire et des FSC, ont appuyé un chiffrement robuste… [et] se sont opposés à des mesures visant un "accès exceptionnel" (comme une clé [de déchiffrement] sous condition ou des "portes dérobées" techniques)[329] ».

328 Gouvernement du Canada, *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*, 19 mai 2017.
329 Sécurité publique Canada, « Summary of Notable Submissions on Lawful Access », ébauche, sans date.

144. Également en mai 2017, spécialement en réponse au livre vert, le Comité permanent de la sécurité publique et nationale (SECU) a déposé un rapport intitulé *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale au Canada*. Le comité SECU recommandait de ne pas donner suite aux dispositions concernant le chiffrement ou l'accès aux RBA[330]. Dans sa réponse publique faisant suite au rapport, le gouvernement a donné son accord en ce qui a trait au chiffrement en indiquant qu'il était « dans l'intérêt du Canada de s'assurer que les technologies de chiffrement sont éprouvées et utilisées à grande échelle », et que « [a]lors que l'expansion du chiffrement a eu pour effet de mettre en évidence des lacunes importantes pour les organismes chargés de l'exécution de la loi et de la sécurité nationale, le gouvernement ne considère pas que des réponses législatives élaborées en fonction de ces difficultés soient viables. Le gouvernement continue d'examiner des options afin de s'assurer que les ministères et les organismes ont les ressources nécessaires pour accéder aux données déchiffrées requises afin de prévenir des attentats terroristes et de réagir aux activités criminelles[331]. » La réponse ne faisait pas état de la recommandation du SECU à l'encontre d'une loi portant sur les RBA.

145. Le 20 juin 2017, le gouvernement a déposé le projet de loi C-59, la *Loi de 2017 sur la sécurité nationale*, sans aucune disposition ayant trait à l'accès légal[332]. Plus tôt au cours du même mois, Sécurité publique Canada avait informé le ministère de la Justice qu'il avait « quelques inquiétudes » au sujet de la tenue des consultations à venir concernant la capacité d'interception et, dans le même ordre d'idées, a demandé au ministère de la Justice de suspendre toute consultation portant sur les RBA[333].

146. Plus tard, le même mois, le Canada a été l'hôte de la Conférence des cinq nations de 2017 réunissant à Ottawa les ministres de la Sécurité publique ainsi que les procureurs généraux. Dans leur communiqué conjoint, les ministres ont noté que le chiffrement pouvait « grandement compromettre les efforts de sécurité publique en empêchant l'accès légal à la teneur des communications », mais ont convenu que les gouvernements du Groupe des cinq coopéreraient avec les FSC de façon à explorer des solutions partagées « tout en préservant la cybersécurité et les droits et libertés individuels[334]. »

147. L'année suivante, en Australie, les ministres de la Sécurité publique et les procureurs généraux du Groupe des cinq se sont réunis et ont publié l'Énoncé de principes sur l'accès à la preuve et le chiffrement. L'énoncé encourageait les FSC à [traduction] « bien vouloir intégrer des outils d'accès légal à leurs produits », mais indiquait également que les gouvernements pourraient [traduction] « envisager des mesures dans le domaine des technologies, de l'application de la loi, de la législation ou encore d'autres mesures qui permettraient de mettre en œuvre des solutions d'accès légal[335]. »

148. ***[336]

330 Comité permanent de la sécurité publique et nationale, *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale du Canada*, 2 mai 2017.
331 Ministre de la Sécurité publique et de la Protection civile, réponse du gouvernement au rapport du SECU du 2 mai 2017, sans date.
332 Le projet de loi C-59 recevrait la sanction royale en 2019.
333 Ministère de la Justice, « Consultation sur l'accès aux renseignements sur les abonnés », 9 juin 2017.
334 Gouvernements de l'Australie, du Canada, des États-Unis, de la Nouvelle-Zélande et du Royaume-Uni, « Réunion ministérielle des cinq pays 2017 : Communiqué conjoint », 27 juin 2017.
335 Gouvernements de l'Australie, du Canada, des États-Unis, de la Nouvelle-Zélande et du Royaume-Uni, « Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019 », 30 juillet 2019, mis à jour le 23 octobre 2019.
336 ***

149. En juin 2019, le SECU a déposé le rapport intitulé *Cybersécurité dans le secteur financier comme un enjeu de sécurité nationale*. Le rapport a appuyé la définition de chiffrement fort d'un expert – c'est-à-dire « des algorithmes de chiffrement pour lesquels aucune faiblesse ou vulnérabilité n'est connue ou n'a été intégrée[337] » – et a recommandé « que le gouvernement du Canada rejette les approches à l'accès légal qui affaibliraient la cybersécurité[338]. »

150. Le Groupe des cinq a continué de se concentrer sur le chiffrement lors de la réunion suivante tenue en juillet 2019, au R.-U. Le communiqué conjoint de la Conférence des cinq nations indiquait que les FSC [traduction] « devraient intégrer des mécanismes à la conception des produits et des services cryptés selon lesquels les gouvernements disposant des pouvoirs légaux appropriés pourraient accéder aux données requises dans un format qu'il est possible de lire et d'utiliser[339] » pour appuyer les enquêtes et agir contre le contenu illégal.

43e législature (de 2019 à 2021)

151. En octobre 2020, le ministre de la Sécurité publique et de la Protection civile s'est joint à ses homologues des pays du Groupe des cinq, de l'Inde et du Japon pour la publication de la *Déclaration internationale : chiffrement de bout en bout et sécurité publique*[340] pilotée par le R.-U. La Déclaration internationale constituait principalement une réponse à l'annonce de Facebook, faite en mars 2019, concernant son plan de mise en œuvre du chiffrement de bout en bout dans l'ensemble de ses plateformes, notamment dans Facebook Messenger[341]. Cette déclaration indiquait que le chiffrement de bout en bout compliquait les enquêtes de police et minait « la capacité d'une entreprise à cibler les […] cas les plus graves de contenu et d'activité de nature illégale, y compris […] la propagande terroriste et la planification d'attaques [et à intervenir dans de tels cas] ». La déclaration invitait les entreprises à se concentrer « sur des solutions raisonnables et réalisables sur le plan technique » de sorte à permettre de lire et de cibler les contenus illicites se trouvant sur leurs plateformes et de prendre les mesures nécessaires pour faciliter « les enquêtes et les poursuites relatives aux infractions » et d'être en mesure de fournir du « contenu dans un format qu'il est possible de lire et d'utiliser » lorsqu'un mandat a été délivré[342].

152. En novembre 2020, le gouvernement a approuvé un plan permettant au ministre de la Sécurité publique et de la Protection civile de mener des consultations auprès du public et des intervenants dans le but de soutenir l'élaboration d'une position de principe gouvernementale sur le chiffrement de bout en bout et l'accès légal[343]. Les consultations avaient pour objet d'informer le gouvernement au sujet de la façon de répondre au défi posé par le chiffrement dans le cadre de sa stratégie globale visant à promouvoir la prospérité du Canada dans un monde numérique tout en protégeant la vie privée et la sécurité publique[344].

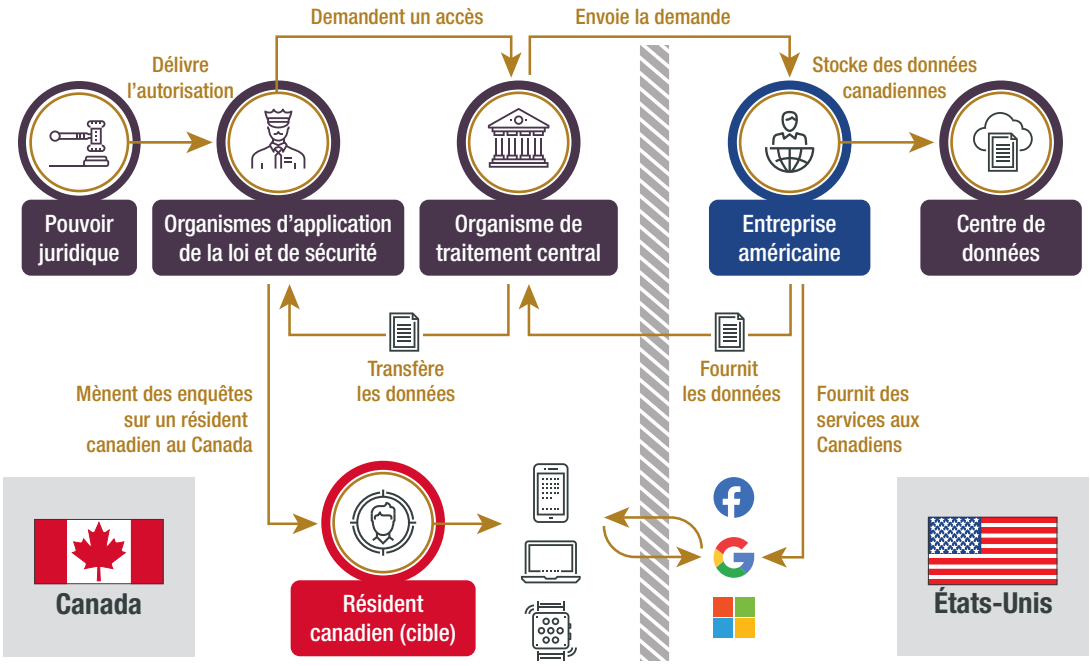
337 Christopher Parsons (associé en recherche, Citizen Lab, Université de Toronto), Témoignages devant le SECU, 27 février 2019, cité dans SECU, *Cybersécurité dans le secteur financier comme un enjeu de sécurité nationale*, juin 2019.
338 SECU, *Cybersécurité dans le secteur financier comme un enjeu de sécurité nationale*, juin 2019.
339 Gouvernements de l'Australie, du Canada, des États-Unis, de la Nouvelle-Zélande et du Royaume-Uni, « Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019 », 30 juillet 2019, mis à jour le 23 octobre 2019.
340 Gouvernements de l'Australie, du Canada, des États-Unis, de l'Inde, du Japon, de la Nouvelle-Zélande et du Royaume-Uni, « Déclaration internationale : chiffrement de bout en bout et sécurité publique », 11 octobre 2020.
341 Mark Zuckerberg, « Privacy-Focused Vision for Social Networking », 6 mars 2019.
342 Gouvernements de l'Australie, du Canada, des États-Unis, de l'Inde, du Japon, de la Nouvelle-Zélande et du Royaume-Uni, « Déclaration internationale : chiffrement de bout en bout et sécurité publique », 11 octobre 2020.
343 CST, « Material for bilat between [CSE] Chief and ISED Assoc. DM Paul Thompson », 21 septembre 2020.
344 CST, « Seeking an Approach on Encryption Consultations with Public Safety », note de breffage pour la chef, sans date.

Selon Sécurité publique Canada, ces consultations n'ont pas eu lieu au bout du compte en raison de la « fatigue des intervenants » et d'une crainte de « conséquences négatives sur les réponses[345] » si les consultations avaient eu lieu.

153. Comme indiqué au chapitre 3, au printemps de 2021, le Canada et les États-Unis ont amorcé les négociations officielles devant mener à un accord sur l'accès aux données en vertu du cadre s'appliquant à la *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) des États-Unis[346]. Un tel accord procurerait aux organismes d'application de la loi et de sécurité l'autorisation requise pour demander des données, notamment le contenu des communications, directement auprès des FSC de l'autre pays[347], comme le montre la figure 4.1 ci-après. À ce jour, les É.-U. ont conclu des accords avec le R.-U. en 2019 et avec l'Australie en 2021[348]. Un accord entre le Canada et les États-Unis permettrait au Canada de signifier une ordonnance d'un tribunal canadien directement aux entreprises américaines relativement à des données stockées ou à des interceptions, dans la mesure où l'ordonnance du tribunal canadien ne « vise pas intentionnellement » un Américain ou une personne aux États-Unis, et les entreprises ne commettraient « aucun acte illicite » en obtempérant ainsi aux demandes du Canada[349]. L'inverse s'appliquerait également, c'est-à-dire qu'une demande des États-Unis ne pourrait pas viser intentionnellement un Canadien ou une personne au Canada. ***[350]

345 Ministre de la Sécurité publique, comparution devant le CPSNR, 5 novembre 2024.
346 Le Canada et les États-Unis ont annoncé les négociations en mars 2022. Les États-Unis mènent aussi des négociations avec l'Union européenne et la Nouvelle-Zélande en vue de conclure des accords similaires. Gouvernements du Canada et des États-Unis, « United States and Canada Welcome Negotiations of a CLOUD Act Agreement », communiqué de presse, 22 mars 2022; et Sécurité publique Canada, « Negotiations Status Update – Canada-US Data Access Agreement », présentation pour le ministre, novembre 2023.
347 Sécurité publique Canada, « US CLOUD Act: DMNS », 22 février 2019.
348 Département de la Justice des États-Unis, « CLOUD Act Resources », page Web, consultée en octobre 2024.
349 CLOUD Act des États-Unis, articles 104 et 105, respectivement.
350 Ministère de la Justice, « Department of Justice Response to Request for Information #3 », 15 novembre 2024.

Figure 4.1 : Accords bilatéraux au titre du cadre de la CLOUD Act des États-Unis[351]



44e législature (de 2021 à novembre 2024)

154. En juin 2022, la réponse du gouvernement à une question soumise par écrit au sujet du Feuilleton sur la surveillance électronique a informé la Chambre des communes concernant l'utilisation insoupçonnée d'outils d'enquête sur appareil (OEA) par la GRC, ce qui a donné lieu à une étude du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI). En novembre 2022, le Comité permanent a déposé son rapport intitulé *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*. L'ETHI a formulé plusieurs recommandations voulant, notamment, que le gouvernement modifie la *Loi sur la protection des renseignements personnels* de sorte à obliger les institutions du gouvernement à réaliser des évaluations des facteurs relatifs à la vie privée avant d'utiliser les outils technologiques à risque élevé et à soumettre le résultat de ces évaluations au Commissariat à la protection de la vie privée pour analyse. Le gouvernement a répondu qu'il était déjà en train de mener un examen de la *Loi sur la protection des renseignements personnels*[352].

155. L'ETHI a également recommandé que le gouvernement du Canada mette sur pied un organe consultatif indépendant composé d'intervenants pertinents de la communauté juridique, du gouvernement, de la police et de la sécurité nationale, de la société civile ainsi que des organismes de réglementation pertinents afin d'examiner les nouvelles technologies utilisées par les organismes d'application de la loi et d'établir des normes nationales concernant leur utilisation. Le gouvernement a répondu que la GRC avait instauré le Programme

351 Sécurité publique Canada, « U.S. CLOUD Act: DMNS Presentation », 22 février 2019.
352 Présidente du Conseil du Trésor, « Lettre au président du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique », novembre 2022.

national d'intégration des technologies ayant pour objet de mettre en œuvre un processus central interne capable d'évaluer les nouveaux outils technologiques d'enquête, tout en étudiant les questions relatives à la vie privée et à la loi. L'ETHI a aussi recommandé que le gouvernement du Canada dresse une liste de fournisseurs de logiciels espions interdits. Dans sa réponse, le gouvernement reconnaissait le besoin de se doter de règles claires s'appliquant aux technologies de surveillance, mais n'a pas répondu spécifiquement à la recommandation favorisant le recours à une liste en dehors du régime normal d'exportation.

156. En mars 2023, Sécurité publique Canada a repris les discussions stratégiques sur l'accès légal en faisant un exposé devant le CSMSN. Selon Sécurité publique Canada, rien de particulier n'a déclenché la reprise des discussions sur la question. Ses représentants ont indiqué que [traduction] « le travail stratégique sur l'accès légal ne s'est jamais arrêté sur le plan opérationnel » et reconnaissant que « les préoccupations grandissantes relatives aux lacunes dans la trousse des outils d'enquête *** ont joué un rôle[353] ». Dans le cadre de son exposé, Sécurité publique Canada a fait le point sur les enjeux pertinents et a demandé le point de vue des participants en vue d'un plan stratégique permettant de prendre des mesures à leur égard. Les enjeux étaient les suivants : l'accès aux RBA, l'accès aux métadonnées, l'interception, l'exploitation de réseau informatique et la coopération internationale. Sécurité publique Canada a proposé trois éléments essentiels d'une éventuelle démarche : créer les conditions de réussite en comblant les lacunes en matière de transparence, de crédibilité et de coordination; mettre en œuvre des propositions législatives, par exemple, des exigences en matière de capacité à l'égard des FSC; et *** aboutir à la signature et à la ratification du *Deuxième Protocole additionnel à la Convention sur la cybercriminalité* du Conseil de l'Europe[354].

157. Contrairement au livre vert de 2016, la discussion stratégique renouvelée sur l'accès légal n'a pas abordé la conservation des données. Selon Sécurité publique Canada, il [traduction] « surveille l'élaboration de politiques sur la conservation de données à l'étranger depuis 2016 » et « la conservation des données fait toujours partie de la discussion stratégique sur l'accès légal aujourd'hui », le travail stratégique se concentrant sur des « réformes législatives possibles ***[355]. »

158. En mai 2023, le Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN)[356] a tenu une réunion avec des représentants de la société civile, du milieu universitaire et de ministères et organismes de la sécurité nationale sous le thème « Technologies émergentes et outils numériques pour la protection de la sécurité nationale ». Selon le compte rendu, des experts de Sécurité publique Canada ont informé les membres du GCT-SN de l'élaboration

353 Sécurité publique Canada, « NSICOP Lawful Access RFI #3 to Public Safety », 15 novembre 2024.
354 Sécurité publique Canada, « Digital Investigative Capabilities: Renewal of the Lawful Access Policy Development Agenda », présentation au CSMSN, 22 mars 2023.
355 Sécurité publique Canada, « NSICOP Lawful Access RFI #3 to Public Safety », 15 novembre 2024.
356 En juillet 2019, le ministre de la Sécurité publique et de la Protection civile a annoncé la création du Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN) pour mettre en œuvre l'engagement de transparence de 2017 du gouvernement en matière de sécurité nationale. Le GCT-SN, un organe indépendant et externe, est composé d'anciens fonctionnaires, d'universitaires et de membres de la société civile. Son rôle est de conseiller le sous-ministre de la Sécurité publique sur « les mesures à prendre pour intégrer la transparence dans les politiques, les programmes et les activités du Canada en matière de sécurité nationale de manière à accroître la responsabilité démocratique et la sensibilisation du public. » GCT-SN, « La numérisation de la sécurité nationale : technologie, transparence et confiance », juillet 2024.

d'un cadre sur la transparence en matière de capacités d'enquête numériques (soit la capacité des organismes de sécurité d'accéder aux informations des cibles conservées par les FSC)[357]. Le résumé de la réunion ne comprend aucune recommandation sur la voie à suivre.

159. C'est en juin 2023 que le Canada a signé le *Deuxième Protocole additionnel à la Convention sur la cybercriminalité* du Conseil de l'Europe, lequel prévoit « […] une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaines et pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés, des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic, la coopération immédiate en cas d'urgence, des outils d'entraide, mais aussi des garanties en matière de protection des données à caractère personnel[358]. » Après la signature du *Deuxième Protocole additionnel* par le Canada, le ministère de la Justice a mené des consultations avec les intervenants, y compris les provinces et territoires, et des commissaires à la protection de la vie privée[359]. La consultation demandait « le type d'autorisation (par exemple, judiciaire ou autre) que le Canada devrait exiger » pour que les enquêteurs de l'étranger obtiennent différents types de données auprès des FSC canadiens et « si le Canada devrait refuser d'autoriser l'accès direct » par des enquêteurs de l'étranger « aux renseignements sur les abonnés détenus par les [FSC] canadiens. » Le Commissariat à la protection de la vie privée du Canada estime que le Canada devrait refuser et que la mise en œuvre au Canada du *Deuxième Protocole additionnel* devrait obliger l'obtention d'une ordonnance d'un tribunal canadien pour toutes les demandes de l'étranger[360].

160. Comme l'indique le chapitre 2, en mars 2024, la Cour suprême a conclu à la majorité dans l'affaire *R. c. Bykovets* qu'il existait également une attente raisonnable en matière de vie privée liée à l'adresse IP d'une personne[361]. En réponse à cette décision, des représentants du ministère de la Justice ont réexaminé [traduction] « la question de l'accès légal aux renseignements sur les abonnés et se sont penchés sur des solutions possibles afin de répondre à certaines difficultés de l'accès légal à court et à moyen terme[362]. » Le ministre de la Justice a indiqué qu'il était ouvert à étudier la possibilité de mettre en place un seuil des motifs raisonnables de soupçonner pour les RBA[363].

161. En juillet 2024, le GCT-SN a publié un rapport intitulé *La numérisation de la sécurité nationale : technologie, transparence et confiance*[364]. Le rapport faisait état de préoccupations concernant le manque de transparence de l'appareil de la sécurité nationale

357 Gouvernement du Canada, « Compte rendu de la réunion du Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN) 26 et 27 mai 2023 », 18 avril 2024.

358 En septembre 2024, 45 États – dont le Canada – avaient signé, mais non ratifié, le Deuxième Protocole additionnel, et deux États l'avaient ratifié. Conseil de l'Europe, « Détails du traité nº 224 », consulté le 2 octobre 2024; et Conseil de l'Europe, « État des signatures et ratifications du traité 224 », consulté le 2 octobre 2024.

359 Ce n'était pas la première fois que le gouvernement mobilisait les intervenants sur la question. Commissariat à la protection de la vie privée du Canada (CPVP), « Mémoire du Commissariat à la protection de la vie privée du Canada à l'intention du ministère de la Justice Canada – Objet : Document de consultation sur le Deuxième Protocole additionnel à la Convention de Budapest », 22 mars 2024; ministère de la Justice, « Deuxième protocole additionnel sur la cybercriminalité », page Web, dernière modification le 21 février 2024; et ministère de la Justice, « Conseil de l'Europe Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques : Consultations, 2023 », présentation tirée de la page Web.

360 CPVP, « Mémoire du Commissariat à la protection de la vie privée du Canada à l'intention du ministère de la Justice Canada – Objet : Document de consultation sur le Deuxième Protocole additionnel à la Convention de Budapest », 22 mars 2024.

361 *R. c. Bykovets*, 2024 CSC 6.

362 Ministère de la Justice, « Department of Justice Response to Request for Information #3 », 15 novembre 2024.

363 Ministère de la Justice, comparution devant le CPSNR, 7 novembre 2024; et ministère de la Justice, « Department of Justice Response to Request for Information #3 », 15 novembre 2024.

364 GCT-SN, « La numérisation de la sécurité nationale : technologie, transparence et confiance », juillet 2024.

et du renseignement en matière de gestion des données et son utilisation des métadonnées. Il a également soulevé des préoccupations sur la position du gouvernement en matière de chiffrement, indiquant que « si le chiffrement doit être affaibli aux fins de la sécurité nationale, en le rendant déchiffrable ou au moyen de portes dérobées, un certain nombre de mesures de protection devront être mises en place, notamment la diffusion rapide, voire automatique, d'information au public sur les atteintes et la surveillance étroite et le signalement de leur utilisation par les organismes d'application de la loi[365] ». Le rapport demande au gouvernement de renseigner les Canadiens « sur les besoins en matière de capacités de déchiffrement de la police ou des services de renseignement de sécurité et les risques connexes » et de fournir des « justifications pleinement intelligibles […] pour les décisions politiques en matière de cryptographie, [qui] devraient inclure des renseignements complets sur l'incidence réelle du chiffrement sur la sécurité nationale, bien au-delà de mots à la mode tels que "devenir invisible"[366]. »

162. Au mois de novembre 2024, le Canada et les États-Unis poursuivent les négociations devant donner lieu à un accord entre ces deux pays sur l'accès aux données, ***[367] ***[368] ***[369]. En juillet 2024, le ministre de la Sécurité publique ainsi que le ministre de la Justice se sont réunis avec leurs homologues américains à Washington, D.C. Le secrétaire à la Justice des États-Unis a indiqué qu'il y avait consensus quant à la majeure partie de l'accord, tout en signalant quelques questions à résoudre. Le ministre de la Justice a quant à lui rappelé que le Canada souhaitait conclure l'accord, soulignant que les questions problématiques pouvaient être résolues[370]. ***[371]

163. En octobre 2024, l'ETHI a déposé le rapport *Utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et ordinateurs*, qui portait sur les appareils fournis par le gouvernement. Bien qu'il ne portât pas précisément sur l'accès légal, le rapport a réitéré cinq recommandations que l'ETHI avait formulées dans son étude de 2022 sur l'utilisation d'outils d'enquête sur appareil par la GRC, y compris la recommandation voulant que le gouvernement modifie la *Loi sur la protection des renseignements personnels* pour obliger les institutions gouvernementales à réaliser des évaluations des facteurs relatifs à la vie privée avant d'utiliser des outils technologiques à risque élevé et à présenter les évaluations au Commissariat à la protection de la vie privée aux fins d'examen[372].

365 GCT-SN, « La numérisation de la sécurité nationale : technologie, transparence et confiance », juillet 2024.
366 GCT-SN, « La numérisation de la sécurité nationale : technologie, transparence et confiance », juillet 2024.
367 ***
368 Ministre de la Sécurité publique, comparution devant le CPSNR, 5 novembre 2024.
369 Ministre de la Justice, comparution devant le CPSNR, 7 novembre 2024; et ministère de la Justice, « Justice Response for Factual Accuracy », 20 décembre 2024.
370 Sécurité publique Canada, courriel de mise à jour destiné aux dirigeants de Sécurité publique Canada et du ministère de la Justice de la part du conseiller de Sécurité publique Canada (agent de liaison) à l'ambassade du Canada à Washington, D.C. concernant le Forum sur la criminalité transfrontalière de 2024, 24 juillet 2024.
371 Ministre de la Justice, comparution devant le CPSNR, 7 novembre 2024.
372 ETHI, *Utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et ordinateurs*, 10 octobre 2024. Le 4 novembre 2024, le gouvernement n'avait toujours pas présenté une réponse.

Chapitre 5 : Évaluation

164. Lorsqu'il a entrepris le présent examen sur l'accès légal aux communications par les organismes de sécurité et de renseignement, le Comité a décidé de répondre à trois grandes questions :

- Les défis d'accès légal du Canada sont-ils aussi préoccupants pour les enquêtes sur la sécurité nationale que le prétendent les organismes de sécurité et de renseignement?
- Le gouvernement a-t-il réussi à trouver des solutions à ces défis ou à les atténuer?
- De quelle manière le gouvernement du Canada facilite-t-il ou permet-il la tenue d'enquêtes sur la sécurité nationale tout en protégeant le droit des Canadiens à la vie privée?

165. Dans le cadre de l'examen, le Comité s'est entretenu avec deux ministres et 33 représentants de cinq ministères et organismes, dont des administrateurs généraux et des enquêteurs en sécurité nationale. Étant conscient que ces comparutions ne représentaient que la perspective du gouvernement, le Comité a également sollicité les points de vue d'avocats de la défense, d'experts en cybersécurité et en droit, de défenseurs de la vie privée et de groupes de la société civile. En outre, le Comité a recueilli les commentaires de fournisseurs de services de communication (FSC) canadiens. Enfin, le Comité s'est appuyé sur des exposés classifiés et a consulté des documents gouvernementaux des douze dernières années, des publications universitaires, des articles dans les médias, des baladodiffusions, des blogues ainsi que des rapports portant sur des sujets semblables réalisés par des démocraties aux vues similaires.

166. Dans le cadre de son évaluation, le Comité se penche sur l'importance des défis d'accès légal du Canada ainsi que sur la réponse du gouvernement face à ces défis sur les plans opérationnel et stratégique, tout en tenant compte de la relation entre la sécurité nationale et le droit des Canadiens à la vie privée.

Évaluation des défis d'accès légal du Canada

167. Le Comité a appris que les organismes de sécurité et de renseignement du Canada font régulièrement face à des défis dans le cadre d'enquêtes sur des menaces envers la sécurité nationale en raison des répercussions combinées de l'évolution rapide de la technologie, de la nature mondiale des communications numériques ainsi que d'un cadre juridique qui n'évolue pas au même rythme que les avancées technologiques. Bien que ces avancées technologiques aient offert de nouvelles possibilités au SCRS et à la GRC dans le cadre de la collecte d'information à l'appui de leurs mandats respectifs, les deux organisations ont indiqué que, actuellement, les défis excèdent les possibilités. Le Comité a constaté que les répercussions et l'importance de chacun de ces défis varient pour chaque organisation, selon la mesure dans laquelle le SCRS ou la GRC est en mesure de les atténuer. On aborde cette dynamique ci-dessous.

Technologie

168. Le Comité n'a pas observé de données claires et empiriques démontrant les défis importants d'accès légal auxquels les organismes de sécurité et de renseignement du Canada affirment faire face en raison de l'évolution rapide de la technologie. Le SCRS et la GRC ne consignent pas systématiquement la fréquence à laquelle ils font face à des difficultés technologiques dans le cadre d'enquêtes sur la sécurité nationale, par exemple des situations où ils n'auraient pas pu accéder à des communications, car elles étaient chiffrées. Par conséquent, ils ne sauraient quantifier les répercussions et l'importance réelles de ces défis. Pour cette raison, le Comité ne disposait d'aucune donnée à analyser pour dégager les tendances au fil du temps. Il s'agit d'une omission importante, car ces organisations informent le gouvernement et tentent de convaincre les Canadiens (surtout ceux concernés par une possible atteinte à leur vie privée) qu'il faut mettre en place de nouvelles dispositions législatives et des ressources pour suivre le rythme de l'évolution de la technologie, mais sont seulement en mesure de fournir des anecdotes et non des données concrètes.

169. De hauts fonctionnaires de Sécurité publique Canada, du SCRS et de la GRC ont indiqué à plusieurs reprises que dans les situations où le SCRS et la GRC n'étaient pas en mesure d'accéder au contenu de communications, ils ont trouvé d'autres moyens d'obtenir l'information recherchée. Toutes les organisations ont indiqué que les métadonnées, lorsqu'elles sont connues, disponibles et suffisamment précises, sont également utiles dans le cadre d'enquêtes, ce qui confirme que le SCRS et la GRC ne perdent pas l'accès aux informations, mais qu'ils se heurtent à ce que le Citizen Lab qualifie de « friction[373] » dans le cadre des enquêtes.

170. Cependant, le Comité a entendu un témoignage détaillé et convaincant concernant la façon dont le rythme rapide des changements technologiques a augmenté la complexité, le risque opérationnel et les coûts des enquêtes sur la sécurité nationale. Un plus grand nombre d'appareils numériques, d'applications de communication et de systèmes d'exploitation signifie que les enquêteurs ont besoin de trouver des méthodes d'accès supplémentaires, ce qui a une incidence sur le temps et les ressources. L'ERI est dispendieuse et n'est pas toujours efficace (voir ci-dessous). D'autres mesures d'atténuation *** d'accéder au contenu de communications chiffrées*** sont maintenant complexes***. (Le Comité note qu'aucun organisme de sécurité et de renseignement n'a soulevé de préoccupation concernant l'intelligence artificielle du point de vue de l'accès légal, outre le fait qu'une utilisation accrue de l'intelligence artificielle pourrait appuyer la préparation de rapports médico-légaux.)

171. En résumé, malgré le fait que le SCRS et la GRC n'ont pas systématiquement recueilli de données sur les défis technologiques rencontrés pendant la période visée par l'examen, le Comité croit tout de même disposer de suffisamment d'information pour confirmer qu'ils ont bel et bien de la difficulté à accéder aux renseignements et aux éléments de preuve numériques en temps opportun.

373 Lex Gill, Tamir Israel et Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.

C1	Les organismes de sécurité et de renseignement du Canada ne consignent pas systématiquement la fréquence à laquelle ils font face à des difficultés technologiques dans le cadre d'enquêtes sur la sécurité nationale, et s'ils ont pu pallier ces difficultés.
C2	La GRC et le SCRS ont de la difficulté à accéder au contenu de communications, que les métadonnées ne peuvent pas nécessairement remplacer.

R1	Sous la direction du ministre de la Sécurité publique, le gouvernement élabore et met en œuvre une stratégie exhaustive visant à remédier aux défis d'accès légal du Canada, en s'appuyant sur l'examen et les conclusions du Comité. La stratégie devrait : • établir les principes clés, comme la légitimité, la nécessité et la proportionnalité; • cerner et consigner les principaux défis d'accès légal et les risques connexes et en rendre compte; • comprendre des communications, la mobilisation des intervenants et des engagements en matière de transparence; • prendre en compte les défis que peuvent poser les technologies émergentes, par exemple l'intelligence artificielle.

172. L'utilisation très répandue du chiffrement représente un dilemme important. Après avoir examiné la réponse stratégique du gouvernement au chiffrement, malgré les défis grandissants dans le cadre des enquêtes sur la sécurité nationale, le Comité estime que la décision du gouvernement en 2020 de ne pas aller de l'avant avec de nouvelles consultations sur le chiffrement était raisonnable, car il était en effet peu probable que le point de vue des principaux intervenants ait changé depuis les consultations sur la sécurité nationale menées par Sécurité publique Canada en 2016. Le Comité constate que presque aucun travail stratégique concerté sur le chiffrement n'a été réalisé depuis. Les ministères et les organismes fédéraux semblent s'être entendus sur une position de travail interne commune : le chiffrement est essentiel dans une société qui se veut numérique par défaut, et toute mesure visant à dégrader son intégrité n'est pas compatible avec la cybersécurité. Il convient de noter qu'aucun fonctionnaire n'a indiqué au Comité vouloir qu'une loi obligeant la création d'un accès exceptionnel ou d'une porte dérobée pour contourner le chiffrement soit mise en place.

173. Les déclarations publiques du gouvernement à ce jour portent toutefois à confusion. La signature par le Canada du communiqué conjoint de la Conférence des cinq nations sur le chiffrement de 2019 et de la *Déclaration internationale : chiffrement de bout en bout et sécurité publique* pilotée par le R.-U. peut porter à croire que le gouvernement envisage toujours une telle mesure législative. En effet, le rapport publié récemment, à l'été 2024, par le Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN) dans lequel il dit s'inquiéter qu'il s'agisse de la position du gouvernement, alors que le Comité n'a aucun doute que ce n'est pas le cas, porte à croire qu'il serait important de fournir des explications publiquement compte tenu des préoccupations du public en matière de cybersécurité et de vie privée.

174. Selon le Comité, lorsque le gouvernement exposera la position du Canada sur le chiffrement, il devra expliquer clairement que ***accéder au contenu de communications chiffrées est bien plus qu'une simple « friction » dans les enquêtes. Le Comité a été informé que l'ERI ne constitue pas une panacée, et que l'accès aux métadonnées connexes n'est pas équivalent à l'accès au contenu de communications en temps réel. Par conséquent, le Comité estime que de mettre de nouvelles lois et ressources ainsi que de nouveaux outils à la disposition de l'appareil de la sécurité et du renseignement est nécessaire pour atténuer ce risque, mais que ceux-ci doivent faire abstraction du chiffrement.

175. Le Comité a également constaté que les défenseurs de la vie privée et de la cybersécurité ainsi que les praticiens de la sécurité nationale semblent communiquer à sens unique lors des débats sur le chiffrement et l'accès exceptionnel pour les organismes d'application de la loi et de renseignement. À mesure que les intervenants discutent d'initiatives stratégiques et de lois, il sera essentiel que les deux parties s'assurent d'avoir une compréhension commune des principaux concepts. En ce qui concerne le gouvernement, le Comité affirme qu'une stratégie de communication robuste et transparente, dans laquelle on explique des concepts techniques en détail, est essentielle.

C3	Lors des comparutions, il y avait consensus qu'une loi obligeant la création d'un accès exceptionnel ou de portes dérobées sur les plateformes de chiffrement n'était ni nécessaire, ni souhaitée.
C4	La position publique du Canada concernant l'accès légal aux communications chiffrées n'est pas claire. Les praticiens de la sécurité nationale, les experts en cybersécurité et les défenseurs de la vie privée n'ont pas une compréhension commune du problème.

R2	Le gouvernement précise publiquement sa position concernant l'accès exceptionnel à l'information sur les communications protégée par chiffrement.

176. Le Comité a appris que l'utilisation du chiffrement et de technologies d'anonymisation a également une incidence sur la façon dont la GRC et le SCRS peuvent obtenir l'information de base requise au début d'une enquête, ***. À cet égard, le Comité a appris que la décision de la Cour suprême en 2014 dans l'affaire *Spencer* selon laquelle une ordonnance de la cour est requise pour obtenir des RBA a entraîné des retards et demande une augmentation significative des efforts de la part des organismes de sécurité lorsqu'ils enquêtent sur une possible menace envers la sécurité nationale. Les mesures prises par le ministère de la Justice pour résoudre cette question n'ont pas progressé depuis de nombreuses années. En outre, le Comité comprend que l'absence d'un régime entourant la conservation des données a entraîné des conséquences considérables compte tenu de la durée de certaines enquêtes complexes.

C5	L'inaction du gouvernement quant à l'élaboration et à la mise en œuvre d'une solution pour donner suite à la décision de la Cour suprême dans l'affaire *Spencer* nuit à la capacité du SCRS et de la GRC de répondre aux menaces envers la sécurité nationale.
C6	Sans une exigence légale générale obligeant les FSC à conserver des métadonnées pendant une période précise, les données demandées en vertu d'un mandat pourraient ne pas être disponibles.

R3	Le gouvernement présente un projet de loi visant à établir de nouveaux pouvoirs dans la *Loi sur le Service canadien du renseignement de sécurité* et le *Code criminel* permettant la communication de renseignements de base sur les abonnés, et le gouvernement examine un projet de loi concernant la conservation des données.

177. Selon les praticiens de la sécurité et du renseignement, les défenseurs de la vie privée et les experts en cybersécurité, l'ERI, y compris le déploiement d'un outil d'enquête sur appareil (OEA), est une *** solution possible pour accéder au contenu de communications dans le contexte de l'utilisation très répandue du chiffrement. Le Comité a appris que ces outils sont dispendieux et souvent peu fiables, car les cibles sont de plus en plus habiles avec la cybersécurité et les entreprises s'efforcent de cerner et de corriger les vulnérabilités des systèmes d'exploitation et des plateformes de chiffrement ***.

178. Le recours à l'ERI soulève également des questions importantes concernant la protection des techniques d'enquête. Le Comité a appris qu'en raison de la complexité de l'ERI, ***. Le Comité a été informé que la GRC fait face à certaines difficultés quant à l'utilisation d'OEA à l'appui de ses enquêtes, car des *** renseignement canadien *** n'ont pas confiance que le système juridique du Canada saura les protéger adéquatement de la divulgation lors d'instances judiciaires.

179. ***. ***, ainsi que des experts en droit, soutiennent plutôt que des dispositions de la *Loi sur la preuve au Canada* ont permis de protéger de tels renseignements lors de poursuites judiciaires, et avancent qu'il se peut que ce ne soit pas le cadre juridique du Canada qui pose problème, mais plutôt une aversion pour le risque institutionnelle. Le Comité a également été informé que, pour répondre aux menaces envers la sécurité nationale, il se pourrait que les poursuites judiciaires ne constituent pas le moyen le plus efficace, et que la perturbation sans poursuite pourrait être plus viable lorsqu'il est question de techniques sensibles.

180. Tandis que la technologie continue de changer et de gagner en complexité, le Comité suppose que les organismes de sécurité et de renseignement du Canada ***. Le SCRS et le CST semblent être à l'abri, car le risque de divulgation est faible, mais le Comité s'inquiète que la capacité de la GRC *** soit limitée. Le Comité convient que, dans certains cas, la perturbation est une réponse plus prudente à une menace envers la sécurité nationale, mais ne dispose d'aucune information qui porte à croire que les Canadiens préfèrent un système juridique où les organismes d'application de la loi ont régulièrement recours à la perturbation plutôt qu'à la poursuite en réponse à une menace envers la sécurité nationale.

181. Le Comité fait remarquer que cette difficulté est un aspect perpétuel du débat plus vaste et de longue durée au sujet du dilemme entourant le renseignement et la preuve au Canada. Le Comité s'inquiète que, comme le débat sur le chiffrement, cette question ait également atteint une impasse. Le Comité est conscient qu'il n'existe pas de solution simple au défi de l'utilisation de renseignements, ou d'outils et de techniques sensibles, dans le cadre d'une poursuite criminelle; et souligne les efforts déployés par le SCRS et la GRC pour améliorer la coopération et la collaboration par le biais du Projet d'amélioration des opérations de 2019. Toutefois, peu importe si le problème est de nature législative ou découle d'une aversion pour le risque institutionnelle, le Comité estime que la lenteur à laquelle le gouvernement aborde le problème lié au renseignement et à la preuve d'un point de vue stratégique entraîne des conséquences imprévues sur la primauté du droit au Canada en ce qui concerne la réponse aux menaces envers la sécurité nationale.

C7	L'incapacité du gouvernement de faire progresser le dilemme entourant le renseignement et la preuve, surtout en ce qui concerne la protection des techniques d'enquête, a contribué à mettre la GRC dans une situation où elle doit choisir entre ne pas pouvoir utiliser d'outils et de techniques sensibles dans le cadre d'une enquête en raison des possibles enjeux de divulgation, ou risquer de ne pas pouvoir s'appuyer sur des éléments de preuve obtenus par le biais de ces outils et techniques devant les tribunaux, ou qu'une poursuite soit suspendue en raison d'une ordonnance de divulgation.

R4	Pour donner suite à la recommandation du Comité en 2024 dans son *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada*, à savoir que le gouvernement s'emploie à résoudre les difficultés liées au renseignement et à la preuve, le gouvernement élabore et met en œuvre une solution visant à répondre aux préoccupations concernant la protection des outils d'enquête, ce qui pourrait nécessiter la modification des dispositions pertinentes de la *Loi sur la preuve au Canada.*

182. En plus de se pencher sur le besoin pressant d'améliorer la protection des techniques d'enquête, le Comité estime que de plus amples travaux stratégiques doivent être réalisés concernant l'utilisation d'OEA. Le Comité était satisfait d'apprendre que le SCRS et la GRC veillent à ce que les mandats autorisant l'installation et l'utilisation d'OEA contiennent plusieurs mesures de protection en matière de vie privée. Toutefois, le Comité constate l'absence d'une orientation stratégique sur l'achat d'OEA commerciaux destinés aux organismes d'application de la loi et de renseignement, au-delà de l'exigence générale de réaliser une évaluation des facteurs relatifs à la vie privée. Le Comité estime qu'une politique serait également nécessaire pour aborder les préoccupations en matière de transparence entourant l'utilisation d'OEA, notamment en ce qui concerne la complexité du processus de demande de mandat.

C8	Le gouvernement ne dispose pas de politiques officielles sur l'achat, la réglementation et l'utilisation d'outils d'enquête sur appareil commerciaux, ainsi que sur la production de rapports transparents concernant leur utilisation par les organismes d'application de la loi et le SCRS.

R5	Le gouvernement élabore des politiques et des lignes directrices concernant l'achat et l'utilisation d'outils d'enquête sur appareil commerciaux, ainsi que sur les exigences en matière de production de rapports à cet égard.

Absence de législation régissant la capacité d'interception

183. Le Comité a appris que, contrairement à plusieurs démocraties aux vues similaires, le Canada ne dispose pas de législation obligeant les FSC à développer, à déployer et à maintenir leurs systèmes de sorte qu'ils conservent une capacité d'interception. Pendant la période visée par l'examen, le SCRS et la GRC ont plutôt eu recours à une approche volontaire, ***. Ces risques comprennent des retards, une ambiguïté sur le plan juridique, des inefficacités financières et ***. Cette situation remet également en cause la capacité du Canada de collaborer avec des partenaires aux vues similaires qui disposent de cadres régissant la capacité d'interception.

184. Le Comité a également appris que l'absence d'une autorité centrale pour la coordination des initiatives d'interception légale, le triage des demandes et la normalisation des approches pour tous les organismes de sécurité nationale et d'application de la loi a été source de confusion et de frustration pour toutes les parties. Le Comité constate que le SCRS et la GRC ont réalisé des progrès quant à la création d'un Centre national pour l'accès légal, mais se demande pourquoi ce fut aussi long et pourquoi les efforts pour trouver une solution à ce défi d'accès légal semblent en si grande partie s'opérer de bas en haut.

185. Tous les représentants des FSC ont fait part de leurs préoccupations au Comité concernant le manque de législation, notamment en ce qui concerne l'absence d'un cadre d'indemnisation clair pour les services judiciairement autorisés qui sont offerts par les FSC. Le Comité constate également que, sans l'élaboration d'une politique officielle dirigée par Sécurité publique Canada ou discussions connexes menées par les ministres au Cabinet, la GRC et le SCRS ont mis en place des principes informels, qui ont orienté leurs politiques, leurs procédures et leurs pratiques. À ce jour, ces principes étaient tous adaptés de façon à assurer une collaboration continue de la part des FSC, notamment la question entourant un cadre d'indemnisation du gouvernement, s'il en est, pour les services rendus par les FSC. La question consistant à déterminer si les coûts liés au respect de la loi devraient être pris en charge par les FSC ou par le gouvernement doit faire l'objet de discussions au Cabinet, et éventuellement de débats au Parlement.

C9	L'absence de législation imposant aux fournisseurs de services de communication (FSC) de maintenir une capacité d'interception légale entraîne des risques inutiles pour tous les intervenants, y compris le SCRS, les organismes d'application de la loi fédéraux, provinciaux, territoriaux et municipaux, les FSC et, au bout du compte, la population canadienne. Elle fait également obstacle à la capacité du Canada de collaborer avec ses partenaires internationaux. Le fait de ne pas régler cette question sur le plan stratégique a poussé les organisations opérationnelles à élaborer elles-mêmes des politiques et des procédures fondamentales, notamment un modèle d'indemnisation, visant à assurer une coopération continue de la part des FSC, à défaut d'une approche fondée sur des principes et orientée par les commentaires des ministres et du Parlement.
C10	Les risques associés à l'absence d'une législation obligeant les fournisseurs de services de communication à maintenir une capacité d'interception sont accentués par l'absence d'une autorité nationale centralisée qui coordonne, élabore et maintient les capacités d'interception légale au Canada.

R6	Le gouvernement dépose une loi obligeant les fournisseurs de services de communication (FSC) à maintenir une capacité d'interception. La législation doit être neutre sur le plan du chiffrement et ne doit pas comporter d'exigence de déchiffrement. Le gouvernement doit également établir un modèle d'indemnisation pour les coûts liés au respect de la loi, c'est-à-dire qu'il doit déterminer si les FSC doivent être indemnisés pour les coûts d'élaboration, de maintenance et de fonctionnement liés à l'accès légal. La législation doit : • mettre en place et désigner l'autorité nationale (c'est-à-dire le Centre national pour l'accès légal) pour la coordination des initiatives d'interception légale; • définir le terme « fournisseur de services de communication » pour s'assurer d'inclure tout fournisseur de services qui mène des activités au Canada et qui offre des services ou des capacités de communication électronique; • définir la capacité d'interception de façon à inclure un soutien à l'exploitation de réseau informatique; • établir des normes techniques obligatoires, notamment en ce qui a trait à la cybersécurité.

Obstacles sur le plan des compétences

186. Le Comité a été informé de la façon dont les flux transfrontaliers d'information numérique entravent les enquêtes sur la sécurité nationale, un enjeu devenu particulièrement problématique puisqu'un nombre croissant de Canadiens utilisent des applications et des services de communication établis dans d'autres pays. Cette dynamique n'est pas récente, et le Canada a pris d'importantes mesures pour se joindre à des efforts internationaux visant à remédier aux obstacles sur le plan des compétences, notamment par la signature et la ratification de la *Convention de Budapest sur la cybercriminalité* du Conseil de l'Europe, et par la signature plus récente du *Deuxième Protocole additionnel*. Le Canada et les États-Unis négocient également un accord sur l'accès aux données en vertu de la *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) des États-Unis. Une fois conclu, cet accord neutre sur le plan du chiffrement permettrait d'éliminer des obstacles de longue date sur le plan des compétences empêchant l'accès autorisé par les tribunaux aux FSC des États-Unis, y compris les grandes plateformes de médias sociaux. Cet accord est particulièrement important pour le SCRS, qui ne peut avoir recours au processus d'entraide juridique dont se sert la GRC. Le Canada bénéficierait grandement de cet accord.

187. Le Comité est préoccupé par le temps nécessaire au Canada et aux États-Unis pour négocier cet accord. Le Comité observe que depuis l'adoption de la CLOUD Act en 2018, les États-Unis ont conclu des accords avec le R.-U. et l'Australie en 2019 et 2021 respectivement. ***le Comité s'inquiète que le gouvernement se rende compte qu'il a raté une occasion de finaliser un accord si les États-Unis décident d'accorder la priorité à d'autres pays pour conclure des accords d'accès aux données.

C11	L'accord sur l'accès aux données entre le Canada et les États-Unis permettrait de surmonter des obstacles de longue date sur le plan des compétences qui empêchent l'accès judiciairement autorisé aux fournisseurs de services de communication des États-Unis, y compris les grandes plateformes de médias sociaux, et ce, sans compromettre le droit à la vie privée ou le chiffrement.

R7	Le gouvernement priorise la signature et la mise en œuvre de l'accord sur l'accès aux données entre le Canada et les États-Unis.

Évaluation de la réponse du gouvernement

188. Le Comité constate que même si les gouvernements qui se sont succédé étaient conscients de ces difficultés, ils ont été en grande partie inefficaces dans l'élaboration de réponses par le biais de solutions stratégiques ou de modifications législatives. Le gouvernement n'a déployé aucun effort valable pour se pencher sur l'accès légal depuis les consultations tenues dans le contexte du livre vert de 2016, lors desquelles les Canadiens ont clairement exprimé leurs préoccupations concernant des propositions visant à résoudre les difficultés de l'accès légal. Le Comité aurait considéré la réponse du gouvernement comme étant raisonnable s'il avait poursuivi les travaux stratégiques visant à élaborer des solutions qui respectent tant les préoccupations liées à la protection de la vie privée que le besoin de mettre des outils et des ressources modernes à la disposition des organismes de sécurité.

189. Toutefois, le Comité estime que, plutôt que de réévaluer la voie à suivre, le gouvernement a laissé des initiatives stratégiques importantes stagner. D'abord, la Cour suprême a rendu sa décision dans l'affaire *Spencer* concernant les RBA il y a plus de dix ans. Le gouvernement n'a soumis aucune proposition pour régler la question des RBA. Ensuite, aucun gouvernement n'a tenté de remédier à l'absence d'une législation régissant la capacité d'interception légale depuis 2012. De plus, les tentatives du gouvernement d'élaborer une politique cohérente sur le chiffrement ont peu progressé. Enfin, les négociations concernant un accord sur l'accès aux données indispensable entre le Canada et les États-Unis ont progressé lentement, sans sentiment d'urgence.

190. L'effet cumulatif de cette approche de l'accès légal est que le Canada ne peut suivre le rythme des démocraties aux vues similaires, qui ont progressé il y a plus de dix ans en adaptant leurs cadres juridiques pour lutter contre les menaces envers la sécurité nationale à l'ère numérique. Dans un contexte mondial où le Canada devra de plus en plus travailler avec ses partenaires internationaux pour lutter contre l'extrémisme violent à caractère idéologique, le crime organisé grave, la cybercriminalité, l'ingérence étrangère et d'autres menaces, le Canada est désavantagé.

191. Le Comité estime que cette inertie juridique et stratégique se résume à un manque de volonté politique. L'accès légal ne figurait dans aucune lettre de mandat depuis que le gouvernement a commencé à les rendre publiques, ce qui porte le Comité à croire que le gouvernement n'est pas convaincu de l'importance et de l'incidence des défis de l'accès légal du Canada. Le Comité fait remarquer la complexité des défis de l'accès légal, qui couvrent le croisement entre la technologie qui évolue rapidement, les points de vue changeants sur la vie privée, les cadres juridiques et la jurisprudence, ainsi que les initiatives stratégiques distinctes, mais

interreliées. Les aspects de l'accès légal se rapportent les uns aux autres, de sorte qu'on doit tenir compte de plusieurs implications avant de déterminer la voie à suivre. Le Comité soupçonne que cette complexité en soi a également contribué aux années d'inertie.

192. Le Comité estime également que la situation actuelle pourrait refléter la difficulté du gouvernement à communiquer efficacement avec les Canadiens qui sont préoccupés par la protection de leur vie privée.

Observations du Comité concernant le débat sur la sécurité nationale et le droit à la vie privée des Canadiens

193. Le Comité est d'accord avec la déclaration du commissaire à la protection de la vie privée qu'il est possible de respecter la vie privée et la sécurité nationale simultanément, plutôt que de respecter l'une au détriment de l'autre. Le Comité est encouragé de constater qu'aucun des témoins ayant comparu dans le cadre du présent examen n'a dépeint l'équilibre entre la protection de la vie privée et la sécurité nationale comme étant un jeu à somme nulle. Les défenseurs de la vie privée ont reconnu que, dans certains cas, les organismes de sécurité doivent accéder à des communications privées à l'appui de leurs enquêtes sur la sécurité nationale. Les praticiens de la sécurité nationale ont régulièrement souligné la nécessité que leurs activités de surveillance électronique soient conformes à la Charte, qu'elles contribuent à un objectif légitime et qu'elles soient nécessaires et proportionnées. Tous ont convenu qu'il était inutile de réduire le débat à une dichotomie entre les Canadiens qui appuient « Big Brother » et ceux qui sont en faveur de la protection de la vie privée. Selon le Comité, il y a donc lieu que les principaux intervenants tiennent une discussion fondée sur des principes concernant la voie à suivre.

194. Pour ce faire, le Comité estime qu'il sera important pour le gouvernement de réduire l'écart entre ce que les Canadiens *supposent* que les organismes de sécurité et de renseignement sont en mesure de faire et la réalité. Le Comité est conscient que la GRC et le SCRS ne veulent pas et, dans certains cas, ne peuvent pas communiquer publiquement de l'information concernant les techniques d'enquête et les vulnérabilités opérationnelles. Le Comité croit que la justification de limiter cette information dans la sphère publique est en grande partie raisonnable. Toutefois, le vide d'information créé peut perpétuer des suppositions inexactes voulant que les organismes de sécurité et de renseignement disposent de capacités et de ressources supérieures à la réalité. Le Comité croit que, même si les affirmations concernant un « âge d'or de la surveillance » étaient vraies il y a dix ans, elles ne reflètent pas entièrement les défis actuels auxquels les praticiens de la sécurité nationale font face.

195. Néanmoins, le Comité croit que la modernisation de la législation régissant l'accès légal est une question pour laquelle la transparence concernant les capacités et les détails techniques sera importante pour dissiper les suppositions erronées et répondre aux préoccupations en matière de cybersécurité et de protection de la vie privée. Si le gouvernement veut réaliser des progrès importants relativement à la réforme de l'accès légal, il ne pourra pas miser sur des points de discussion généraux lorsqu'il collabore avec les principaux intervenants. Le Comité remarque que des démocraties aux vues similaires ont réalisé des progrès à cet

égard, surtout le Royaume-Uni qui a rédigé, adopté et récemment revu la *Investigatory Powers Act*. Il existe des approches en matière de transparence fondées sur des principes dont le Canada peut s'inspirer.

196. Le Comité pense également que la GRC et le SCRS pourraient améliorer la façon dont ils interprètent les préoccupations des Canadiens quant à la protection de la vie privée, et dont ils y répondent. Par exemple, le Comité a constaté que le SCRS et la GRC mettent régulièrement de l'avant les autorisations judiciaires et la complexité du processus de demande de mandat comme preuve que les préoccupations en matière de protection de la vie privée ont été abordées dans le contexte de l'utilisation de techniques d'accès légal. Le Comité fait observer que cette réponse, bien que raisonnable, pourrait ne pas être efficace, car elle ne décrit pas explicitement *comment* les organisations ont évalué les préoccupations en matière de protection de la vie privée. Un autre exemple est lorsque la British Columbia Civil Liberties Association a cité la décision rendue par la Cour fédérale en 2016 concernant l'obligation de franchise du SCRS, ce dernier a répondu qu'il avait depuis rétabli la confiance de la Cour. Selon le Comité, là n'est pas la question. Il s'agit plutôt de rétablir la confiance des Canadiens qui ont des préoccupations quant à la protection de leur vie privée, ce sur quoi le SCRS doit encore travailler.

197. Enfin, le Comité fait état de l'observation de M. Goold selon laquelle les défenseurs de la vie privée sentent qu'ils doivent « être sur la défensive » lorsque le gouvernement envisage de moderniser la législation régissant l'accès légal. Le Comité estime que si le gouvernement veut faire progresser la réforme de l'accès légal, l'un des principaux piliers de sa stratégie devrait consister à déterminer la façon de nouer le dialogue et de communiquer efficacement avec les Canadiens, particulièrement ceux qui ont des préoccupations relativement à la protection de la vie privée et à la Charte, en cherchant à cerner les situations où les deux parties communiquent à sens unique, et à y remédier de façon proactive.

Conclusion

198. L'accès légal représente l'un des pouvoirs les plus intrusifs de l'État pour la protection de la sécurité nationale. Par conséquent, les Canadiens s'attendent à ce qu'on encadre son utilisation au moyen de mesures de protection rigoureuses, notamment à ce qu'elle soit prescrite par la loi, qu'elle contribue à un objectif légitime et qu'elle soit nécessaire et proportionnée. À juste titre, les Canadiens veulent comprendre toute proposition de nouveaux outils et pouvoirs pour les organismes de sécurité et de renseignement qui ont une incidence sur la protection de leur vie privée. Toutefois, les Canadiens s'attendent également à ce que les organismes de sécurité et de renseignement disposent des outils, des politiques et des autorisations légales pour employer des techniques d'accès légal. Le Comité croit également que les Canadiens seraient surpris d'apprendre à quel point il est difficile pour ces organismes de le faire.

199. En réfléchissant à l'information apprise tout au long de l'examen, le Comité est préoccupé par les défis d'accès légal décrits par l'appareil de la sécurité et du renseignement ainsi que par l'incapacité persistante des gouvernements qui se sont succédé à y faire face. La GRC et le SCRS ne perdent peut-être pas entièrement accès aux informations, mais ce n'est pas grâce aux nouvelles technologies et à une abondance de métadonnées qui compensent la perte d'accès au contenu de communications. Les deux organisations semblent plutôt atténuer les difficultés liées aux technologies de chiffrement, à un cadre juridique désuet et aux limites sur le plan des compétences en gérant, pour l'instant, la complexité et le risque opérationnels accrus. Le Comité s'inquiète toutefois de la mesure dans laquelle cette atténuation dépend de l'ingéniosité du SCRS et de la GRC ou s'appuie sur le bon agencement d'outils, d'autorisations légales et de ressources.

200. Le Comité s'inquiète tout autant que, si l'on ne surmonte pas ces défis, elles pourraient porter atteinte à la sécurité nationale du Canada à long terme en entravant de plus en plus la capacité du SCRS et de la GRC à remplir leurs mandats respectifs. Le défaut de répondre à ces défis pourrait également nuire à la capacité continue du Canada de tirer parti des efforts du Groupe des cinq visant à détecter les menaces envers la sécurité et à y répondre s'il ne peut pas contribuer de manière significative à ce partenariat.

201. Le Comité est d'avis que la principale façon dont le gouvernement pourrait faciliter et favoriser les enquêtes sur la sécurité nationale tout en protégeant le droit des Canadiens à la vie privée serait de moderniser la législation régissant l'accès légal, en se fondant sur des principes énoncés clairement qui réitèrent la nécessité d'un besoin légitime pour l'accès exceptionnel, ciblé et autorisé par les tribunaux; mettent l'accent sur les mesures de protection en matière de vie privée et de cybersécurité; et définissent les mécanismes de surveillance et de transparence. Compte tenu de la complexité des défis de l'accès légal, le Comité suggère que le gouvernement emploie une approche graduelle permettant une mobilisation significative des intervenants et une contribution diversifiée.

202. Cependant, il est essentiel que le gouvernement se penche sur ces questions de manière proactive. Il existe plusieurs exemples à l'échelle internationale de démocraties aux vues similaires qui ont adopté de manière précipitée des lois régissant l'accès légal controversées en réponse à des incidents graves de sécurité nationale. Les parlementaires devraient avoir la possibilité de participer au débat sur de nouvelles mesures législatives régissant l'accès légal de manière réfléchie et avec perspicacité, et non de manière précipitée et émotive en réponse à une tragédie nationale. Plus ces questions sont reléguées au second plan, plus le gouvernement expose le Canada au risque de faire face à la même situation.

203. Il ne s'agit pas de nouvelles difficultés; les gouvernement qui se sont succédé en étaient conscients depuis un certain temps. Il est temps pour le gouvernement d'agir et de fournir à l'appareil de la sécurité et du renseignement les outils, les politiques et les autorisations légales dont il a besoin pour faire ce qu'on lui demande, de la façon attendue par les Canadiens, c'est-à-dire en tenant compte de leur vie privée et en la protégeant.

Conclusions du Comité

204. Le Comité formule les conclusions suivantes.

C1	Les organismes de sécurité et de renseignement du Canada ne consignent pas systématiquement la fréquence à laquelle ils font face à des difficultés technologiques dans le cadre d'enquêtes sur la sécurité nationale, et s'ils ont pu pallier ces difficultés.
C2	La GRC et le SCRS ont de la difficulté à accéder au contenu de communications, que les métadonnées ne peuvent pas nécessairement remplacer.
C3	Lors des comparutions, il y avait consensus qu'une loi obligeant la création d'un accès exceptionnel ou de portes dérobées sur les plateformes de chiffrement n'était ni nécessaire, ni souhaitée.
C4	La position publique du Canada concernant l'accès légal aux communications chiffrées n'est pas claire. Les praticiens de la sécurité nationale, les experts en cybersécurité et les défenseurs de la vie privée n'ont pas une compréhension commune du problème.
C5	L'inaction du gouvernement quant à l'élaboration et à la mise en œuvre d'une solution pour donner suite à la décision de la Cour suprême dans l'affaire *Spencer* nuit à la capacité du SCRS et de la GRC de répondre aux menaces envers la sécurité nationale.
C6	Sans une exigence légale générale obligeant les FSC à conserver des métadonnées pendant une période précise, les données demandées en vertu d'un mandat pourraient ne pas être disponibles.
C7	L'incapacité du gouvernement de faire progresser le dilemme entourant le renseignement et la preuve, surtout en ce qui concerne la protection des techniques d'enquête, a contribué à mettre la GRC dans une situation où elle doit choisir entre ne pas pouvoir utiliser d'outils et de techniques sensibles dans le cadre d'une enquête en raison des possibles enjeux de divulgation, ou risquer de ne pas pouvoir s'appuyer sur des éléments de preuve obtenus par le biais de ces outils et techniques devant les tribunaux, ou qu'une poursuite soit suspendue en raison d'une ordonnance de divulgation.
C8	Le gouvernement ne dispose pas de politiques officielles sur l'achat, la réglementation et l'utilisation d'outils d'enquête sur appareil commerciaux, ainsi que sur la production de rapports transparents concernant leur utilisation par les organismes d'application de la loi et le SCRS.

C9	L'absence de législation imposant aux fournisseurs de services de communication (FSC) de maintenir une capacité d'interception légale entraîne des risques inutiles pour tous les intervenants, y compris le SCRS, les organismes d'application de la loi fédéraux, provinciaux, territoriaux et municipaux, les FSC et, au bout du compte, la population canadienne. Elle fait également obstacle à la capacité du Canada de collaborer avec ses partenaires internationaux. Le fait de ne pas régler cette question sur le plan stratégique a poussé les organisations opérationnelles à élaborer elles-mêmes des politiques et des procédures fondamentales, notamment un modèle d'indemnisation, visant à assurer une coopération continue de la part des FSC, à défaut d'une approche fondée sur des principes et orientée par les commentaires des ministres et du Parlement.
C10	Les risques associés à l'absence d'une législation obligeant les fournisseurs de services de communication à maintenir une capacité d'interception sont accentués par l'absence d'une autorité nationale centralisée qui coordonne, élabore et maintient les capacités d'interception légale au Canada.
C11	L'accord sur l'accès aux données entre le Canada et les États-Unis permettrait de surmonter des obstacles de longue date sur le plan des compétences qui empêchent l'accès judiciairement autorisé aux fournisseurs de services de communication des États-Unis, y compris les grandes plateformes de médias sociaux, et ce, sans compromettre le droit à la vie privée ou le chiffrement.

Recommandations

205. Le Comité formule les recommandations suivantes.

R1	Sous la direction du ministre de la Sécurité publique, le gouvernement élabore et met en œuvre une stratégie exhaustive visant à remédier aux défis d'accès légal du Canada, en s'appuyant sur l'examen et les conclusions du Comité. La stratégie devrait : • établir les principes clés, comme la légitimité, la nécessité et la proportionnalité; • cerner et consigner les principaux défis d'accès légal et les risques connexes et en rendre compte; • comprendre des communications, la mobilisation des intervenants et des engagements en matière de transparence; • prendre en compte les défis que peuvent poser les technologies émergentes, par exemple l'intelligence artificielle.
R2	Le gouvernement précise publiquement sa position concernant l'accès exceptionnel à l'information sur les communications protégée par chiffrement.
R3	Le gouvernement présente un projet de loi visant à établir de nouveaux pouvoirs dans la *Loi sur le Service canadien du renseignement de sécurité* et le *Code criminel* permettant la communication de renseignements de base sur les abonnés, et le gouvernement examine un projet de loi concernant la conservation des données.
R4	Pour donner suite à la recommandation du Comité en 2024 dans son *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada*, à savoir que le gouvernement s'emploie à résoudre les difficultés liées au renseignement et à la preuve, le gouvernement élabore et met en œuvre une solution visant à répondre aux préoccupations concernant la protection des outils d'enquête, ce qui pourrait nécessiter la modification des dispositions pertinentes de la *Loi sur la preuve au Canada*.
R5	Le gouvernement élabore des politiques et des lignes directrices concernant l'achat et l'utilisation d'outils d'enquête sur appareil commerciaux, ainsi que sur les exigences en matière de production de rapports à cet égard.

R6	Le gouvernement dépose une loi obligeant les fournisseurs de services de communication (FSC) à maintenir une capacité d'interception. La législation doit être neutre sur le plan du chiffrement et ne doit pas comporter d'exigence de déchiffrement. Le gouvernement doit également établir un modèle d'indemnisation pour les coûts liés au respect de la loi, c'est-à-dire qu'il doit déterminer si les FSC doivent être indemnisés pour les coûts d'élaboration, de maintenance et de fonctionnement liés à l'accès légal. La législation doit : • mettre en place et désigner l'autorité nationale (c'est-à-dire le Centre national pour l'accès légal) pour la coordination des initiatives d'interception légale; • définir le terme « fournisseur de services de communication » pour s'assurer d'inclure tout fournisseur de services qui mène des activités au Canada et qui offre des services ou des capacités de communication électronique; • définir la capacité d'interception de façon à inclure un soutien à l'exploitation de réseau informatique; • établir des normes techniques obligatoires, notamment en ce qui a trait à la cybersécurité.
R7	Le gouvernement priorise la signature et la mise en œuvre de l'accord sur l'accès aux données entre le Canada et les États-Unis.

Annexes

Annexe A : Cadre de référence

Examen

Examen du cadre de l'interception légale des communications par les organismes de sécurité et de renseignement conformément à l'alinéa 8(1)a) de la Loi sur le CPSNR.

Aperçu

Selon le ministère de la Justice, l'accès légal consiste en l'interception autorisée de communications ainsi qu'en la collecte d'informations et de données utilisées par les organismes de renseignement et les services de police dans le cadre d'enquêtes. Les organismes de renseignement et les services de police disposent déjà d'importants pouvoirs et capacités d'accès autorisé, mais le maintien de cet accès dans un environnement où la technologie évolue rapidement constitue un défi de taille.

Selon de nombreuses sources ouvertes, l'appareil de la sécurité nationale et du renseignement fait face à des défis croissants en ce qui a trait à sa capacité d'intercepter des communications ou d'accéder au contenu de ces communications, et ce, même lorsque le pouvoir légal de le faire existe. Ce problème est communément appelé « going dark » (perte d'accès aux informations) par les services de police et organismes de sécurité et de renseignement, et résulte de la prévalence et de la sophistication croissantes du chiffrement de bout en bout, ainsi que d'autres changements technologiques qui rendent les solutions d'interception existantes inapplicables.

Or, des groupes de défense des droits civils et des groupes d'intérêt du milieu de la sécurité remettent en question les efforts déployés par le gouvernement pour moderniser les pouvoirs dans ce domaine, soutenant qu'une telle modernisation violerait le droit à la vie privée des Canadiens ou pourrait compromettre la sécurité des données en ligne.

Objectifs

Comme il est indiqué dans la lettre envoyée aux ministres de la Justice, de la Défense nationale et de la Sécurité publique, l'examen portera sur le cadre législatif, réglementaire, stratégique et financier, et ses limites, en matière d'interception légale des communications par les organismes de sécurité et de renseignement, et sur les défis que présentent les technologies nouvelles et émergentes, y compris le chiffrement de bout en bout.

Les objectifs de l'examen consistent à examiner :

- l'état actuel de l'accès légal, y compris les défis cernés par l'appareil de la sécurité nationale et du renseignement;
- les préoccupations et les critiques soulevées par des experts de la société civile et de la protection de la vie privée au sujet de la modernisation des pouvoirs dans ce domaine;

- les défis technologiques liés à l'interception légale des communications, y compris le chiffrement de bout en bout et l'accès aux réseaux de communication en temps réel;
- la mesure dans laquelle l'appareil de la sécurité et du renseignement a atténué les défis de la perte d'accès aux informations au moyen de la technologie, de politiques et de la coopération avec les fournisseurs de services de communication;
- la mesure dans laquelle des lacunes subsistent pour faire face à l'incidence des technologies nouvelles et émergentes sur l'interception légale des communications;
- L'examen portera, sans toutefois s'y limiter, sur le Service canadien du renseignement de sécurité, le Centre de la sécurité des télécommunications, Sécurité publique Canada, la Gendarmerie royale du Canada et le ministère de la Justice.

Comparutions

Quand le Comité aura reçu les documents préliminaires, il tiendra des audiences dont le contenu sera déterminé par les résultats de l'examen préliminaire de ces documents.

Calendrier

Le Secrétariat et le Comité établiront les échéances pour chaque étape de l'examen.

Annexe B : Liste de témoins

Ministres

- L'honorable Dominic LeBlanc, C.P., député, ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales
- L'honorable Arif Virani, C.P., député, ministre de la Justice et procureur général du Canada

Service canadien du renseignement de sécurité

- Directeur
- Directeur général, Services techniques et scientifiques
- Sous-directeur général, Lutte contre le terrorisme
- Sous-directeur général, Services techniques et scientifiques
- Sous-directeur général, Services techniques et scientifiques
- Chef adjoint, Services techniques et scientifiques
- Directeur général, Politique et Relations extérieures

Centre de la sécurité des télécommunications

- Directeur général, ***
- Directeur général, ***

Ministère de la Justice

- Sous-ministre délégué
- Sous-ministre adjoint délégué, Secteur des politiques
- Avocat, Sous-section des services juridiques, CST
- Avocat, Groupe litiges et conseils en sécurité nationale, SCRS
- Avocat, Sous-section des services juridiques, GRC

Commissariat à la protection de la vie privée du Canada

- Commissaire à la protection de la vie privée du Canada
- Sous-commissaire et avocat général principal
- Chef de cabinet, conseillère principale et avocate
- Directeur exécutif, Politiques, Recherche et Affaires parlementaires

Sécurité publique Canada

- Sous-ministre
- Sous-ministre adjoint principal, Sécurité et Cybersécurité nationale
- Directeur, Politiques du renseignement, Sécurité et Cybersécurité nationale
- Gestionnaire intérimaire, Politiques du renseignement, Sécurité et Cybersécurité nationale
- Conseiller principal en politiques, Politiques du renseignement, Sécurité et Cybersécurité nationale

Gendarmerie royale du Canada

- Sous-commissaire, Police fédérale
- Sous-commissaire, Services de police spécialisés
- Surintendant principal, Services d'enquêtes techniques
- Directeur administratif intérimaire, Opérations techniques
- Directeur, Programme de la CLOUD Act
- Sergent, Liaison en matière d'accès légal
- Sergent, Programme technique de gestion des cas
- Analyste des politiques, Services de police spécialisés

Témoins non gouvernementaux

- Six fournisseurs de services de communication canadiens
- Ronald Deibert, directeur, The Citizen Lab, Munk School of Global Affairs & Public Policy, Université de Toronto
- Michael Geist, professeur, Faculté de droit, Université d'Ottawa
- Benjamin Goold, professeur, Allard School of Law, Université de la Colombie-Britannique
- Aislin Jackson, avocate-conseil en politiques, British Columbia Civil Liberties Association
- Anil K. Kapoor, Kapoor Barristers
- Vivek Krishnamurthy, professeur agrégé de droit et directeur de la Samuelson-Glushko Technology Law and Policy Clinic, University of Colorado Law School

Annexe C : Acronymes et abréviations

BCCLA	British Columbia Civil Liberties Association
Charte	*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*, ch. 11 (R.-U.)
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act* (États-Unis)
Convention de Budapest	*Convention de Budapest sur la cybercriminalité* (Conseil de l'Europe)
CPSNR, ou le Comité	Comité des parlementaires sur la sécurité nationale et le renseignement
CPVP	Commissariat à la protection de la vie privée du Canada
CSC	Cour suprême du Canada
CSMSN	Comité des sous-ministres sur la sécurité nationale
CST	Centre de la sécurité des télécommunications
ERI	Exploitation de réseau informatique
ETHI	Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Chambre des communes)
FPT	fédéral, provincial et territorial
FSC	fournisseur de services de communication
GCT-SN	Groupe consultatif sur la transparence de la sécurité nationale
Groupe des cinq	Australie, Canada, États-Unis, Nouvelle-Zélande et Royaume-Uni
G7	Groupe des Sept : Allemagne, Canada, États-Unis, France, Italie, Japon et Royaume-Uni
IP	protocole Internet
normes du solliciteur général	*Normes d'application du Solliciteur général sur l'interception licite des télécommunications*
OEA ou OEE	outil d'enquête sur appareil ou outil d'enquête embarqué
RBA	renseignements de base sur les abonnées
R.-U.	Royaume-Uni
SCRS	Service canadien du renseignement de sécurité
SECU	Comité permanent de la sécurité publique et nationale (Chambre des communes)
Sécurité publique Canada	ministère de la Sécurité publique et de la Protection civile
SFC	surveillance fondée sur un consentement
SPPC	Service des poursuites pénales du Canada
TEJ	traité d'entraide juridique

Annexe D : Glossaire

Accès légal	L'interception des communications électroniques, ainsi que la fouille et la saisie d'informations électroniques, autorisées par les tribunaux, conformément au cadre juridique du Canada[374].
Adresse de protocole Internet (IP)	Identifiant numérique (adresse logique) attribué aux appareils connectés à un réseau informatique qui utilise le protocole Internet[375].
Chiffrement	Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées[376].
Entreprise canadienne	Entreprise de télécommunication qui relève de la compétence fédérale.[377]
Exploitation de réseau informatique	Outils et techniques qui exploitent les vulnérabilités dans les systèmes ou logiciels pour obtenir subrepticement des données stockées ou passant dans des réseaux de communication***.
Fournisseur de services de communication	Entités qui offrent des services de télécommunications ou une combinaison de services d'information et de médias, de contenu, de divertissement et d'applications sur des réseaux[379].
Internet des objets	Divers dispositifs Web « intelligents » utilisés couramment, comme les moniteurs d'activité personnels, les télévisions et les voitures, qui sont munis de capteur intégrés, de composants électriques et de logiciels qui recueillent des données et de l'information dans l'environnement où ils se trouvent[380].
Métadonnées	Des données sur des données, ou un terme informel pour des données de transmission. Dans le contexte des communications, les métadonnées représentent le qui, où, quand, quoi et avec qui des communications, et non le contenu des communications[381].
Outil d'enquête sur appareil	Terme employé par la GRC pour désigner ses outils d'exploitation de réseau informatique.
Porte dérobée	Moyen non recensé qui permet, discrètement ou anonymement, d'accéder à distance à un ordinateur après avoir contourné les mécanismes d'authentification et s'être donné accès au texte en clair.[382]

374 Industrie Canada, ministère de la Justice et Solliciteur général Canada, *Accès légal — Document de consultation*, 2002.
375 Commissariat à la protection de la vie privée du Canada, « Ce qu'une adresse IP peut révéler à votre sujet », mai 2013.
376 CCC, « Glossaire », sans date.
377 *Loi sur les télécommunications* (L.C. 1993, ch. 38).
378 ***
379 Lawful Access Advisory Committee, « Governance Framework », mai 2024.
380 CCC, « Sécurité de l'Internet des objets (IdO) – ITSAP.00.012 », juillet 2022.
381 Adapté du Home Office du Royaume-Uni, « Fact sheet: communications data », 8 juillet 2016.
382 CCC, « Glossaire », sans date.

Renseignements de base sur l'abonné	Des renseignements relatifs à l'abonnement d'un client à un service de télécommunication, comme son nom, son adresse domiciliaire, son numéro de téléphone, son adresse électronique et son adresse de protocole Internet (IP). Ils ne comprennent pas le contenu des communications.[383]
Réseau privé virtuel	Réseau de communication privé habituellement utilisé au sein d'une entreprise ou par plusieurs entreprises pour communiquer au moyen d'un réseau plus vaste. Les communications par RPV sont habituellement chiffrées ou encodées pour en protéger le trafic contre les utilisateurs du réseau public qui sert de support au RPV en question[384].
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens ou les activités d'une organisation[385].

383 Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016 : Document de contexte*, 2016.
384 CCC, « Glossaire », sans date.
385 CCC, « Glossaire », sans date.

Annexe E : Chronologie des efforts législatifs en matière d'accès légal au Canada depuis 2001

2005	
Projet de loi C-74, *Loi sur la modernisation des techniques d'enquête*	
OBJECTIF :	**RÉSULTAT :**
• Obliger les fournisseurs de services de communication à avoir la capacité d'intercepter les communications sur leurs réseaux, y compris de les déchiffrer. • Permettre aux policiers d'obtenir des renseignements sur les abonnés auprès des fournisseurs de services de communication sans autorisation judiciaire préalable.	• Mort au Feuilleton. • Dissolution du Parlement.

2009	
Projet de loi C-46, ***Loi sur les pouvoirs d'enquête au 21e siècle***	
Projet de loi C-47, ***Loi sur l'assistance au contrôle d'application des lois au 21e siècle***	
OBJECTIF :	**RÉSULTAT :**
Dispositions semblables ou identiques à celles du projet de loi précédent. Ajout : • Nouvelles autorités judiciaires : demande et ordonnance de préservation, ordonnances de transmission et de localisation. • Mandats pour la transmission et la localisation en temps réel. • Mise à jour de la législation sur l'assistance mutuelle.	• Mort au Feuilleton. • Prorogation du Parlement.

2010	
Projet de loi C-50, L*oi visant à améliorer l'accès aux outils d'enquête sur les crimes graves* Projet de loi C-51, ***Loi sur les pouvoirs d'enquête au 21e siècle*** Projet de loi C-52, ***Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention***	
OBJECTIF :	**RÉSULTAT :**
Dispositions semblables ou identiques à celles des projets de loi précédents. Ajout : • Possibilité d'obtenir des ordonnances judiciaires additionnelles en plus de l'autorisation d'interception. • Exigences en matière de rapports et de mesures de protection pour les autorisations judiciaires liées à l'accès légal.	• Mort au Feuilleton. • Dissolution du Parlement.

2012	
Projet de loi C-30, *Loi sur la protection des enfants contre les cyberprédateurs*	
OBJECTIF :	**RÉSULTAT :**
Dispositions semblables ou identiques à celles des projets de loi précédents. Ajout : • Dispositions relatives à la durée maximale des autorités judiciaires.	• Non poursuivi par le gouvernement. • Mort au Feuilleton.

2013	
Projet de loi C-13, ***Loi sur la protection des Canadiens contre la cybercriminalité***	
OBJECTIF :	**RÉSULTAT :**
Dispositions semblables ou identiques à celles du projet de loi précédent. Comprend : • Nouvelles autorités judiciaires : demande et ordonnance de préservation, ordonnances de transmission et de localisation. • Mandats pour la transmission et la localisation en temps réel. • Possibilité d'obtenir des ordonnances judiciaires additionnelles en plus de l'autorisation d'interception. • Exigences en matière de rapports et de mesures de protection pour les autorisations judiciaires liées à l'accès légal. • Dispositions relatives à la durée maximale des autorités judiciaires. • Mise à jour de la législation sur l'assistance mutuelle. Exclut : • Capacité obligatoire pour les fournisseurs de services de communication d'intercepter les communications sur leurs réseaux, y compris de les déchiffrer. • Possibilité pour les forces de l'ordre d'obtenir des renseignements sur les abonnés auprès des fournisseurs de services de communication sans autorisation judiciaire préalable.	• A reçu la sanction royale le 9 décembre 2014. • Entrée en vigueur le 9 mars 2015.

2017	
Projet de loi C-59, ***Loi concernant des questions de sécurité nationale***	
OBJECTIF :	**RÉSULTAT :**
Plusieurs mesures modifiant le cadre de sécurité nationale du Canada. Comprend : • Loi habilitante distincte pour le CST et élargissement du mandat. • Autorisation pour le SCRS concernant la collecte, la conservation et la création d'ensembles de données.	• A reçu la sanction royale le 21 juin 2019. • Entrée en vigueur en phases à partir de juillet 2019.