THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Projet de loi C-22 (*Loi de 2026 sur l'accès légal*)

ASSOCIATION DU BARREAU CANADIEN
SECTIONS DU DROIT PÉNAL, DU DROIT DE LA VIE PRIVÉE ET DE L'ACCÈS À L'INFORMATION, ET L'ÉQUIPE ANTICORRUPTION

Mai 2026

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

AVANT-PROPOS

L'Association du Barreau canadien (ABC) est une association nationale qui représente plus de 40 000 juristes, dont des avocats et avocates, des notaires, des universitaires et des étudiants et étudiantes en droit dans tout le Canada. Elle a pour principaux objectifs d'améliorer le droit et l'administration de la justice.

Le présent mémoire a été rédigé par les sections du droit pénal, du droit de la vie privée et de l'accès à l'information, et l'équipe anticorruption de l'ABC, avec l'aide du service de Représentation du bureau de l'ABC. Le mémoire a été revu par le Comité des politiques, qui en a fait la déclaration publique de la les sections du droit pénal, du droit de la vie privée et de l'accès à l'information, et l'équipe anticorruption de l'ABC.

TABLE DES MATIÈRES

Projet de loi C-22 (*Loi de 2026 sur l'accès légal*)

Projet de loi C-22 *(Loi de 2026 sur l'accès légal)*

I. RÉSUMÉ

Les sections de l'Association du Barreau canadien (ABC) sont heureuses d'avoir l'occasion de formuler des commentaires au sujet du projet de loi C-22 (*Loi de 2026 sur l'accès légal*). Nous apprécions également la bonne foi démontrée par les ministres qui ont mis de côté la version précédente (parties 14 et 15 du projet de loi C-2, la *Loi visant une sécurité rigoureuse à la frontière*) pour qu'elle fasse l'objet d'autres consultations auprès des intervenants. Le processus a permis d'améliorer le projet de loi, mais l'ABC a des préoccupations importantes.

Le projet de loi crée de nouveaux pouvoirs en matière d'application de la loi et de sécurité nationale dans la partie 1 et exige que les fournisseurs de services électroniques créent de nouvelles capacités dans la partie 2. La partie 1 a été rédigée par le ministère de la Justice et la partie 2 a été rédigée par le ministère de la Sécurité publique. Bien que les deux parties concernent le thème de l'« accès légal », elles sont suffisamment distinctes pour que des projets de loi distincts améliorent le débat et la discussion.

En ce qui concerne la partie 1, « Accès aux données et aux renseignements en temps opportun », nous sommes préoccupés par l'équilibre entre le seuil pour l'obtention de renseignements relatifs à l'abonné en fonction de la portée des données qui fait partie de la définition (services et dispositifs). En ce qui concerne la partie 2, qui crée une nouvelle « *Loi sur le soutien en matière d'accès autorisé à de l'information* », nos préoccupations sont nombreuses.

Le gouvernement affirme que le Canada est le seul pays du « Groupe des cinq » à ne pas avoir de loi sur l'« accès légal », ce qui n'est qu'à moitié vrai. En ce qui concerne la partie 1 du projet de loi, le Canada dispose depuis longtemps d'outils modernes pour les organismes d'application de la loi et le Service canadien du renseignement de sécurité afin d'intercepter les communications, de fouiller les locaux et les ordinateurs et d'exiger des renseignements sur les clients auprès de fournisseurs de services. Le Canada ne possède pas de cadre exhaustif exigeant des fournisseurs de services qu'ils soient « prêts à l'interception ». Les mesures prises par d'autres pays, en particulier celles qui portent atteinte à la vie privée, ne constituent pas une justification suffisante. Trois des pays du Groupe des cinq n'ont pas de droits protégés par la Constitution en matière de protection de la vie privée ou de protection contre les fouilles, les perquisitions ou les saisies abusives. Le Royaume-

Uni, l'Australie et la Nouvelle-Zélande n'ont pas de balises constitutionnelles, ce qui donne une plus grande marge de manœuvre pour promulguer des lois sur la surveillance intrusive. Pour le Canada, l'article 8 de la *Charte* doit être au premier plan des préoccupations.

II. PRÉOCCUPATIONS GÉNÉRALES

L'ABC conteste les pratiques législatives qui restreignent le débat et diminuent la mobilisation des intervenants. Dans les résolutions 13-04-M[1] et 25-03-A[2], elle a exhorté le gouvernement à limiter les projets de loi omnibus aux modifications techniques mineures. Le projet de loi C-22 instaure plutôt deux régimes différents en vertu de l'« accès légal » : Modifications apportées par la partie 1 au *Code criminel*[3] [ci-après « le *Code* »] et à la *Loi sur le Service canadien du renseignement de sécurité* [ci-après « la *Loi sur le SCRS* »][4] et au nouveau cadre général de la partie 2. Ces éléments doivent être séparés pour permettre au public et aux parlementaires d'y porter une attention adéquate.

Le gouvernement doit éviter de reporter les définitions et les obligations fondamentales aux règlements futurs. Les lois qui élargissent les pouvoirs du gouvernement doivent être claires pour assurer la prévisibilité juridique et éviter le détournement de la fonction.

III. APERÇU DE L'ACCÈS LÉGAL

Le projet de loi C-22 propose de modifier les pouvoirs existants en matière d'accès légal prévus dans le *Code* et la *Loi sur le SCRS,* exigeant des fournisseurs de services qu'ils autorisent les demandes d'accès légal. Avant d'aborder des dispositions précises, les sections de l'ABC souligneront les préoccupations générales.

A. Absence de preuve de nécessité

Le projet de loi C-22 élargit les pouvoirs en matière d'accès légal tout en réduisant la surveillance judiciaire, ayant une incidence importante sur les droits et libertés individuels et imposant des coûts au secteur privé. De tels changements exigent une preuve solide de nécessité et une incidence proportionnelle sur les droits. Le gouvernement n'a pas fourni la preuve que ces changements sont nécessaires.

---

1 ABC, Résolution 13-04-M, Projets de loi omnibus, en ligne.

2 Résolution 25-03-A de l'ABC, Débat et consultation sur les projets de loi en plusieurs parties, en ligne.

3 *Code criminel*, L.R.C. 1985, ch. C-46 [le *Code*].

4 *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23 [*Loi sur le SCRS*].

Dans les séances d'information sur les projets de loi C-2 et C-22, les fonctionnaires ont mentionné le temps écoulé, les progrès technologiques, la croissance des fournisseurs de services numériques, les normes désuètes du solliciteur général en matière d'application de la loi pour l'interception légale des télécommunications et l'absence de nouvelles lois sur l'accès légal au Canada par rapport aux autres pays du Groupe des cinq. Le gouvernement n'a pas fait état des enquêtes qui sont en fait compromises par les dispositions actuelles ou les limites techniques qui empêchent les fournisseurs de services de respecter les ordonnances d'accès légal. La *Loi sur le SCRS*[5] et le *Code*[6] prévoient tous deux des « ordonnances d'assistance », avec surveillance judiciaire des capacités techniques. Sans preuve de nécessité, ces changements ne devraient pas être mis en œuvre.

B. Élargissement de la portée des pouvoirs en matière d'accès légal

Le projet de loi C-22 élargit considérablement l'accès légal : un plus grand nombre de parties pourraient exiger un accès, un plus grand nombre de renseignements pourraient être exigés, les exigences en matière de capacité technique sont élargies et un plus grand nombre d'entités y seraient assujetties, tandis que le pouvoir judiciaire discrétionnaire est restreint. Cet élargissement ne fait pas l'objet d'une consultation adéquate des principaux intervenants au sujet de son incidence, de sa faisabilité et de sa proportionnalité. Nous constatons que les consultations menées sur le projet de loi C-2 et le projet de loi C-22 ont porté sur la « correction » du projet de loi C-2 plutôt que sur la nécessité et la proportionnalité.

C. Absence de mesures de protection

La partie 1 du projet de loi C-22 réduit la surveillance judiciaire. Les pouvoirs liés à l'ordre de confirmer la fourniture de services n'exigent pas l'obtention d'une autorisation judiciaire préalable, et les agents peuvent imposer une interdiction de divulgation d'une durée allant jusqu'à un an. Lorsqu'il y a une surveillance judiciaire, le seuil est faible (c.-à-d. motifs raisonnables de soupçonner). La partie 2 exige des fournisseurs de services qu'ils appuient la surveillance de l'État en mettant en place des mesures de protection minimales, sans critère de proportionnalité efficace, un appel limité et l'interdiction de divulgation, et autorise les ordonnances sans indemnité, transférant les coûts des organismes chargés de l'application de la loi vers le secteur privé, ce qui rend effectivement les entreprises des agents de l'État.

---

5 *SCRS Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23, art. 22.3.

6 *Code criminel*, L.R.C. 1985, ch. C-46, art. 487.02.

La participation du commissaire au renseignement à l'approbation des arrêtés ministériels dans la partie 2 constitue une amélioration par rapport au projet de loi C-2, mais la combinaison des pouvoirs élargis, d'une transparence limitée et de mesures de protection restreintes crée de graves risques pour les droits et libertés individuels.

D. Conformité à la *Charte*

Les sections de l'ABC estiment que les parties 1 et 2 du projet de loi C-22 risquent de contrevenir à la protection conférée par l'article 8 de la *Charte* contre les fouilles, les perquisitions et les saisies abusives. En particulier, la portée des « renseignements relatifs à l'abonné » peut comprendre des renseignements, qui, selon l'article 8 de la *Charte*, doivent démontrer qu'il existe des soupçons plus que raisonnables. De plus, les dispositions de la partie 1 relatives aux divulgations volontaires semblent ne pas concorder avec les décisions de la Cour suprême dans les arrêts *R. c. Spencer* et *R. c. Bykovets*[7].

IV. PARTIE 1 — ACCÈS AUX DONNÉES ET AUX RENSEIGNEMENTS EN TEMPS OPPORTUN

A. Nouvel ordre de confirmer la fourniture de services

La partie 1 présente l'article 487.0121 du *Code*, permettant à un « agent de la paix ou fonctionnaire public », sans autorisation judiciaire, d'exiger qu'un fournisseur de services de télécommunications confirme « si, oui ou non, il fournit ou a fourni des services de télécommunication à tout abonné ou client ou à tout compte ou identifiant, précisés dans l'ordre ».

Délai minimal insuffisant pour se conformer à l'ordre de confirmer la fourniture de services

Le nouveau paragraphe 487.0121(5) impose un délai de réponse de 24 heures. L'ABC propose d'augmenter ce délai pour le faire passer à 48 ou 72 heures, sauf en cas « d'urgence de la situation », car un délai de 24 heures pourrait être irréaliste pour les petits fournisseurs.

Délai pour l'interdiction de divulgation

Le nouveau paragraphe 487.0121(5) permet également aux agents d'interdire la divulgation de l'ordre pour une période allant jusqu'à un an[8]. L'ABC est d'avis que cette exigence est trop rigoureuse et recommande de diminuer le délai à 90 jours et d'obtenir l'approbation requise du tribunal pour les prolongations. Étant donné que la confirmation de la fourniture des services

---

7 *R. c. Spencer*, 2014 CSC 43, [2014] 2 RCS 212; *R. c. Bykovets*, 2024 CSC 6.

8 Article 158 du projet de loi

peut précéder l'ordonnance de communication, les pouvoirs liés à l'interdiction de divulgation qui s'y rattachent doivent également être fermement limités dans le temps.

Révocation ou modification de l'ordre

Le projet de loi C-22 introduit le paragraphe 487.0121(11) du *Code*, permettant à un juge de révoquer ou de modifier un ordre. Les sections de l'ABC soutiennent qu'un juge devrait être en mesure de révoquer un ordre si, dans l'ensemble des circonstances, l'ordre constitue une atteinte déraisonnable à la vie privée de la personne ou des personnes concernées, lorsque l'agent qui a délivré l'ordre ne peut satisfaire au seuil, ou lorsque la conformité ferait en sorte que des résidents non canadiens enfreignent les lois étrangères.

B. Nouvelle ordonnance de communication des « renseignements relatifs à l'abonné »

La partie 1 du projet de loi crée une « ordonnance de communication des renseignements relatifs à l'abonné » exigeant une autorisation judiciaire fondée sur le simple soupçon que a) une infraction au *Code* ou à toute autre loi fédérale a été commise ou sera commise; b) les renseignements relatifs à l'abonné sont en la possession de la personne ou à sa disposition et faciliteront l'enquête relative à l'infraction. Les « motifs raisonnables de soupçonner » constituent le seuil le plus bas de notre système juridique.

Contrairement aux ordonnances générales de communication, qui précisent les données recherchées, cette ordonnance exige « tous les renseignements relatifs à l'abonné » en la possession du destinataire. La définition de « renseignements relatifs à l'abonné » contenue dans le projet de loi C-2 ne se limite pas aux ordonnances générales de communication associant un identifiant à un suspect, traitant des « renseignements biographiques essentiels » protégés par l'article 8 de la *Charte*[9], révélant « des détails intimes sur le mode de vie et les choix personnels de l'individu[10] ».

La définition de « renseignements relatifs à l'abonné », telle qu'elle est actuellement formulée dans la modification proposée de l'article 487.011 du *Code* soulève des préoccupations quant au

---

9 *R. c. Plant*, 1993 CanLII 70 (CSC), à la page 293 : « protège un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État ».

10 *R. c. Bykovets*, *supra,* 2024 CSC 6, para 51, citant l'arrêt *R c. Plant*, 1993 CanLII 70 (CSC), à la page 293; *R. c. Spencer*, *supra*, para 27.

fait que les renseignements saisis dans le cadre de cette définition peuvent comprendre les « renseignements biographiques essentiels ». Les ordonnances peuvent viser tout type de fournisseur de services, comme les hôtels, les centres médicaux où les « types de services fournis » et les dispositifs utilisés (p. ex., les instruments médicaux, l'équipement de réseau) peuvent révéler des renseignements très personnels et de nature délicate.

Les sections de l'ABC font valoir que la définition de « renseignements relatifs à l'abonné » énoncée à l'article 4 du projet de loi, devrait se limiter aux renseignements qui permettent d'identifier l'abonné ou le client. Si le terme « dispositifs » demeure dans la définition, il devrait se limiter aux dispositifs qui facilitent principalement la communication. Tout renseignement en dehors de ceux-ci, fondé sur de simples soupçons, risque d'enfreindre l'article 8 de la *Charte*.

C. Nouvelle autorisation judiciaire pour les demandes de données de transmission ou de renseignements relatifs à l'abonné d'une entité étrangère

Le nouvel article 487.0181 proposé du *Code* autorise une « demande » (et non une ordonnance) visant une « entité étrangère qui fournit des services de télécommunications au public ». La demande est approuvée par un juge sur la présentation d'une requête par un agent de la paix ou un fonctionnaire public. Le seuil pour la délivrance d'une telle demande représente le faible seuil pour la nouvelle ordonnance de communication de renseignements relatifs à l'abonné (soupçons raisonnables).

Sous réserve des mêmes préoccupations exprimées à l'égard de la nouvelle ordonnance de communication de renseignements relatifs à l'abonné (seuil et portée), nous sommes d'avis que cet article tente de façon créative de dissiper l'incertitude entourant la signification d'ordonnances de communication canadiennes à des entités domiciliées entièrement à l'extérieur du Canada, en s'appuyant sur la collaboration volontaire des entités étrangères, mais il soulève des préoccupations semblables au sujet du faible seuil et de la protection de la vie privée.

D. Délais insuffisants pour demander l'examen des ordonnances

Le projet de loi C-22 raccourcit le créneau au cours duquel les destinataires d'une ordonnance de communication ou d'un ordre de fournir des renseignements peuvent demander à la Cour de modifier ou de révoquer l'ordonnance ou l'ordre. L'article 487.0193 modifié du *Code* s'applique à toutes les ordonnances de communication et réduit le délai d'examen à dix jours ouvrables après la

réception de l'ordonnance (alors qu'il était généralement de 30 jours auparavant). Ce délai est trop court, surtout parce que les décisions de contester une ordonnance de communication exigent un processus interne de transmission aux échelons supérieurs, et que de nombreux fournisseurs de services peuvent ne pas avoir de conseillers juridiques disponibles. Il limite également la possibilité d'engagement avec l'agent ou le procureur qui a délivré l'ordonnance pour éviter une demande de nature judiciaire. Ce changement devrait être supprimé du projet de loi. La possibilité pour un destinataire de demander l'examen d'une ordonnance de communication devrait prendre fin uniquement en même temps que le délai imposé par le juge pour produire les documents. Si un préavis à l'agent est conservé, l'avis par courriel devrait être suffisant et interrompre le délai pour donner du temps pour déposer les documents de la requête.

E. Divulgation volontaire et immunité

Une préoccupation importante des sections de l'ABC concerne le fait qu'il n'est pas nécessaire qu'un agent de la paix ou un fonctionnaire public présente un ordre de fournir des renseignements pour « demander » des renseignements si la personne est légalement en possession des renseignements. Le projet de loi prévoit ensuite : « qu'aucun ordre de fournir des renseignements donné en vertu de l'article 487.0121, qu'aucune ordonnance de communication ou qu'aucun mandat n'est nécessaire pour que l'agent de la paix ou le fonctionnaire public puisse recevoir des renseignements dont une personne […] a la possession légitime et y donner suite, si celle-ci les fournit volontairement sans qu'on lui ait demandé ou est légalement tenue de les fournir, notamment par une loi d'un État étranger[11]. »

Bien que les sections de l'ABC reconnaissent que l'intention déclarée du nouveau paragraphe 487.0195(3) proposé peut-être de préciser que la police peut intervenir en cas d'obtention passive et non sollicitée de « dénonciations » (p. ex., du National Center for Missing and Exploited Children ou d'Échec au crime), il crée également un cadre pour les demandes volontaires informelles courantes qui peuvent concerner les « renseignements biographiques essentiels ». L'octroi présumé de l'immunité supprime de fait le droit à la vie privée inhérent aux renseignements demandés. Il est également difficile de savoir comment la fourniture volontaire de renseignements peut être demandée. Une entreprise peut facilement confondre un « ordre » avec une « demande » de fourniture volontaire de documents, ce qui crée un cadre

11 Article 164 du projet de loi : le nouveau paragraphe 487.0195(3) du *Code*

confus. Essentiellement, cela contourne le contrôle judiciaire dans les situations où il pourrait exister un droit impérieux à la vie privée.

Cet article devrait être restreint pour préciser que la police peut recueillir et utiliser les renseignements a) fournis aux organismes d'application de la loi ou au gouvernement de la propre initiative d'une personne ou d'une organisation, sans qu'il lui soit demandé, ou b) les renseignements qui sont signalés à la police ou à d'autres autorités en vertu d'une obligation légale (comme le signalement obligatoire de documents sur les mauvais traitements sexuels et l'exploitation d'enfants).

F. Renseignements « publics »

Le nouveau paragraphe 487.0195(4) du *Code* indique que les policiers ou les fonctionnaires publics peuvent utiliser des renseignements « accessibles au public », en supposant qu'il n'y a aucune attente en matière de protection de la vie privée. Les forces de l'ordre aux États-Unis ont ignoré la Déclaration des droits en procédant à l'acquisition de données de géolocalisation auprès de courtiers de données et de participants à l'écosystème de la publicité en ligne. On pourrait qualifier ces renseignements comme étant « accessibles au public ». Or, la police ne devrait pas être en mesure de contourner la *Charte* en faisant appel à des courtiers de données[12]. De plus, le réseau clandestin regorge de « sites de fuite » où les pirates informatiques communiquent et vendent des renseignements qui ont été volés illégalement par des tiers. Ces renseignements obtenus illégalement seraient « accessibles au public ». Cet article devrait se limiter aux renseignements qui sont déjà accessibles légalement au public et pour lesquels une personne n'a plus d'attente raisonnable en matière de protection de la vie privée.

G. Urgence de la situation

L'article 167 du projet de loi remplacerait l'article 487.11 du *Code*, permettant aux organismes d'application de la loi de saisir des renseignements relatifs à l'abonné ou des données de transmission et de suivi sans ordonnance, lorsque les conditions d'obtention de ces renseignements et de ces données existent en vertu des dispositions applicables proposées, mais qui, en raison de l'urgence de la situation, ne seraient pas réalisables. Un tel ordre doit comprendre suffisamment de renseignements pour que le fournisseur de services soit convaincu

---

12 Wolfie Christl, Astrid Perry, Luis Fernando Garcia, Siena Anstis et Ron Deibert. « Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech, », *Citizen Lab,* rapport nº 191, Université de Toronto, 9 avril 2026, en ligne, et Lena Cohen, Hudson Hongo. « The Government Uses Targeted Advertising to Track Your Location. Here's What We Need to Do. » (*Electronic Frontier Foundation*, 5 mars 2026) en ligne.

de l'urgence de la situation, surtout lorsque des lois étrangères relatives aux demandes urgentes peuvent s'appliquer.

H. Examen des données informatiques : Conservation et destruction

L'article 156 du projet de loi modernise le libellé de l'article 487 du *Code* de façon à inclure l'examen des données informatiques. Les articles 170 et 171 exempteraient les « données informatiques » des articles 489.1 (« Remise des biens ou rapports ») et 490.81 (« Ordonnance de prise en charge ») du *Code*, ce qui fait craindre que les organismes d'application de la loi puissent les conserver indéfiniment. Les sections de l'ABC recommandent une disposition exigeant la destruction des données saisies après un délai déterminé (p. ex., un an), à moins qu'une prolongation ne soit autorisée par le tribunal. Par ailleurs, les sections de l'ABC proposent de modifier les conditions relatives aux mandats[13] concernant les délais de conservation des données au terme desquels les données doivent être détruites à moins d'avoir obtenu une prolongation du délai.

Bien qu'un examen prolongé puisse être utile dans le cadre d'enquêtes complexes et à long terme (p. ex., infractions d'organisation criminelle en cours, homicides, dossiers non résolus d'agression sexuelle, etc.), la conservation pour une période indéterminée et l'utilisation à durée indéterminée sont inacceptables. Les sections de l'ABC soulignent que le *Code* comprend déjà des dispositions sur la destruction des données informatiques dans le contexte des « ordres de préservation » (voir l'article 487.0194 du *Code*).

I. Modifications à la Loi sur le Service canadien du renseignement de sécurité

Les mêmes préoccupations qui ont été soulevées au sujet des modifications proposées au *Code* s'appliquent, avec plus d'acuité, aux modifications complémentaires apportées à la *Loi sur le SCRS*[14]. Dans les procédures en droit criminel, une fois qu'une personne est accusée, elle a la capacité de faire examiner par un juge l'action de l'État dans le cadre d'un procès. Des réparations en vertu de la *Charte* sont disponibles au moment du procès lorsque les agents ne s'acquittent pas de leurs obligations concernant les pouvoirs intrusifs de l'État. En revanche, les activités menées par le Service canadien du renseignement de sécurité demeurent

13 Paragraphe 156(3) du projet de loi : le nouveau paragraphe 487(2.4) proposé du *Code*.

14 *Loi sur le SCRS*, L.R.C. 1985, ch. C-23.

habituellement inconnues des personnes touchées et font rarement l'objet d'une surveillance judiciaire ex post facto. Tout élargissement de l'accès légal au SCRS devrait toujours faire l'objet d'une surveillance et d'un contrôle judiciaires.

V. PARTIE 2 — LOI SUR LE SOUTIEN EN MATIÈRE D'ACCÈS AUTORISÉ À DE L'INFORMATION

A. Généralités

Les sections de l'ABC sont préoccupées par le fait que la partie 2 du projet de loi C-22, qui crée la *Loi sur le soutien en matière d'accès autorisé à de l'information*, n'a pas été justifiée par le gouvernement comme étant nécessaire ou proportionnelle. Elle confie aux « fournisseurs de services électroniques » le mandat de créer des portes dérobées pour permettre aux forces de l'ordre d'avoir accès aux données, ce qui peut attirer des pirates informatiques, minant ainsi la sécurité publique.

La partie 2 du projet de loi C-8, la *Loi sur la protection des cybersystèmes essentiels*, permet aux organismes de réglementation d'ordonner aux « exploitants désignés » de systèmes essentiels de prendre « toute mesure [nécessaire][15] », y compris potentiellement des failles cachées, ce qui confond les obligations en matière de conformité et les régimes d'accès légal et de cybersystèmes.

Les obligations des « fournisseurs principaux » et le contenu des arrêtés ministériels devraient être limitées afin qu'elles ne puissent pas imposer i) les changements à apporter aux produits ou aux services qu'un fournisseur de services électroniques fournit dans le cours normal des activités, ii) la collecte et la conservation de données en dehors de ce que le fournisseur de services électroniques exige à ses propres fins, et iii) les changements qui auraient une incidence sur la fonctionnalité (y compris la demande d'une fonctionnalité supplémentaire) des produits ou des services offerts par le fournisseur de services électroniques.

B. Définitions et portée (article 2)

La portée de l'application de la partie 2 du projet de loi C-2 repose sur la définition de « service électronique » et de « fournisseur de services électroniques ». Le pouvoir d'exiger une capacité technique d'accès légal s'applique aux fournisseurs de services électroniques. Les définitions générales des « services électroniques » et des « fournisseurs de services électroniques »

15 Partie 2, alinéa 36(1)b) de la *Loi sur la protection des cybersystèmes essentiels*.

pourraient comprendre un éventail beaucoup plus large d'entités qui exercent des activités numériques, y compris des activités de vente au détail, des établissements d'enseignement, des établissements de soins de santé, des bureaux juridiques et des médias. Il serait presque impossible de trouver une entreprise au Canada qui ne crée pas, ne conserve pas ou ne transmet pas de renseignements sous forme électronique.

Les sections de l'ABC craignent que le gouvernement puisse imposer des capacités techniques d'accès légal à tous les aspects de la vie numérique. La définition de fournisseur de services électroniques devrait être strictement limitée à ceux qui fournissent principalement des services de communication au public.

C. Fournisseurs principaux et arrêtés ministériels (articles 5 à 13)

Ces articles permettent au gouvernement d'exiger des fournisseurs de services électroniques qu'ils élaborent, mettent à l'essai, mettent en œuvre, exploitent et surveillent les capacités techniques d'accès légal pour donner accès aux renseignements concernant leurs services électroniques. L'article 5 permet au gouverneur en conseil d'adopter des règlements établissant des capacités techniques d'accès légal pour les « fournisseurs principaux », un sous-ensemble de fournisseurs de services électroniques défini par le gouverneur en conseil dans les règlements subséquents. Les sections de l'ABC sont préoccupées par l'absence de garanties procédurales pour ce nouveau pouvoir élargi. L'article 5 ne prévoit aucune obligation de consulter et aucun critère de proportionnalité. Bien que le paragraphe 5(3) dresse la liste des facteurs à considérer, il n'est pas nécessaire de faire preuve de transparence concernant leur examen.

Un fournisseur de services électroniques peut demander une exemption temporaire, mais autrement, il n'y a pas de processus de surveillance ou d'examen autre que le contrôle judiciaire. Tout pouvoir d'imposer des capacités techniques d'accès légal devrait être accompagné de garanties procédurales proportionnelles.

L'article 5 ne prévoit pas non plus un processus de compensation des coûts découlant de l'imposition de capacités techniques d'accès légal. Si un fournisseur de services électroniques est dépourvu d'une capacité précise, c'est généralement parce qu'il n'en a pas légitimement besoin. Par conséquent, les capacités techniques d'accès légal requises en vertu de l'article 5 sont des capacités et des coûts qui seront généralement engagés uniquement pour faciliter l'accès légal aux renseignements. Il s'agit d'un transfert des coûts d'enquête qui relèvent habituellement des organismes chargés de l'application de la loi vers les fournisseurs de services électroniques du

secteur privé. Les sections de l'ABC s'inquiètent des répercussions sur les fournisseurs de services électroniques et de l'augmentation de l'activité d'accès légal si les organismes chargés de l'application de la loi ignorent les coûts de leurs activités.

Alinéa 5(2)a) — Capacités

En exigeant des fournisseurs qu'ils créent et maintiennent des capacités d'interception ou de production de données, le projet de loi exige qu'il y ait un point d'accès privilégié dans des systèmes autrement sécurisés. La généralité du terme crée une ambiguïté dans l'architecture technique requise : incertitude liée à la conformité pour les petits fournisseurs, pouvoir discrétionnaire réglementaire excessif et évaluation complexe de la conformité.

Bien que le gouvernement ait déclaré que le projet de loi C-22 n'autorise pas les portes dérobées, une simple lecture de l'alinéa 5(2)a) et l'absence de balises indiquent le contraire.

Alinéa 5(2)b) — Dispositifs et équipement

La *Loi sur le soutien en matière d'accès autorisé à de l'information* ne devrait pas permettre au gouvernement, par règlement ou arrêté ministériel, d'exiger l'installation d'un équipement ou de dispositifs précis sur les systèmes des fournisseurs. Les entreprises diligentes doivent avoir une pleine connaissance de tout équipement ou dispositif associé à son infrastructure et avoir un contrôle complet sur celui-ci. L'imposition d'une obligation à durée indéterminée d'installer de l'équipement à des fins de surveillance est déraisonnable et présente des risques importants en matière de cybersécurité pour les fournisseurs de services électroniques.

Alinéa 5(2)c) — Avis donnés au ministre ou à d'autres personnes

Les règlements du gouverneur en conseil et les arrêtés ministériels peuvent exiger des fournisseurs de services électroniques qu'ils informent le ministre ou une autre personne des capacités et de tout dispositif, équipement ou autre. L'ABC s'inquiète du fait que cela reflète les pouvoirs contenus dans la loi du Royaume-Unis sur l'accès légal (*Investigatory Powers Act 2016)*, qui a été considérablement élargie par l'*Investigatory Powers (Amendment) Act 2024*.

Il est tout à fait légitime, et devrait le demeurer, qu'une entreprise apporte des changements à ses systèmes qui a) renforcent la sécurité des renseignements de ses utilisateurs et b) réduisent la capacité de l'entreprise de fournir l'accès aux renseignements des utilisateurs. Bon nombre des applications de messagerie les plus populaires au monde ont instauré le « chiffrement de bout en bout », ce qui améliore la sécurité des données des utilisateurs et implique que les forces de l'ordre n'ont plus accès aux messages textes du fournisseur de services.

Alinéa 5(2)d) — Conservation des catégories de métadonnées

Le projet de loi C-22, contrairement au projet de loi C-2, permet aux fournisseurs principaux et aux fournisseurs de services électroniques assujettis à des arrêtés ministériels de conserver les métadonnées pendant une période allant jusqu'à un an. Le paragraphe 5(4) limite les données conservées, mais les métadonnées comprennent des renseignements très sensibles, comme des données de localisation. Il s'agit d'un élargissement spectaculaire par rapport au projet de loi C-2.

En Europe, la conservation obligatoire des métadonnées a été considérée comme une atteinte aux droits à la vie privée lorsque la Cour européenne de justice a invalidé la *Directive sur la conservation des données* de l'Union européenne (UE) en 2014[16], estimant que la conservation générale et systématique des métadonnées des télécommunications de tous les utilisateurs constituait une atteinte disproportionnée aux droits à la protection de la vie privée et des données. La *Directive* obligeait les États membres à imposer la conservation pendant une période de six à vingt-quatre mois. Au cours des années qui ont suivi, la Cour de justice de l'Union européenne a peu à peu précisé que même si la conservation ciblée liée à des menaces ou à des régions géographiques précises peut être permise, la conservation générale des données de tous les utilisateurs demeure incompatible avec les droits fondamentaux de l'UE. Cette décision sera probablement contestée comme une violation de l'article 8 de la *Charte*.

D. Arrêtés ministériels

L'article 7 permet au ministre de la Sécurité publique et de la Protection civile de délivrer des arrêtés ministériels imposant des obligations aux fournisseurs de services électroniques, semblables aux règlements du gouverneur en conseil, avec certaines garanties procédurales. Il s'agit notamment de tenir compte de l'incidence sur l'administration de la justice, du caractère réalisable pour les fournisseurs de services électroniques et de l'incidence sur les utilisateurs des services. Il faut obtenir l'approbation du commissaire au renseignement, mais les fournisseurs de services concernés n'ont pas le droit de présenter des observations et il n'y a aucune transparence quant aux facteurs pris en compte. Cette absence de critères et de garanties procédurales importantes et proportionnelles est une préoccupation importante pour les sections de l'ABC.

16 *Directive sur la conservation des données* de l'UE, en ligne.

À l'heure actuelle, la police et le SCRS peuvent demander à un juge une « ordonnance d'assistance » pour exiger d'un fournisseur de services de fournir de l'aide dans le cadre d'un mandat, possiblement au moyen d'une ordonnance d'interdiction de divulgation. Ces ordonnances sont adaptées au mandat précis, au fournisseur et à la nature de l'assistance requise. Le juge tiendrait compte de l'incidence de la *Charte* dans la délivrance de l'ordonnance d'assistance. Conformément au *Code* et à la *Loi sur le SCRS,* un juge peut faire nommer un ami de la cour qui examinera l'incidence de l'ordonnance sur des tiers. Les ordonnances d'assistance sont, par définition, assujetties à la surveillance et au contrôle judiciaires. Elles sont effectivement remplacées par des arrêtés ministériels sans surveillance judiciaire.

L'ABC souligne qu'il n'existe aucune preuve selon laquelle les ordonnances d'assistance délivrées en vertu du *Code* ou de la *Loi sur le SCRS* sont inadéquates et recommande que les arrêtés ministériels soient retirés du projet de loi.

E. Vulnérabilité systémique (paragraphes 5(3) et 7(4))

Les règlements du gouverneur en conseil et les arrêtés ministériels prévoient qu'un fournisseur peut ignorer une disposition si le fait de s'y conformer « introduir[ait] une vulnérabilité systémique dans les protections électroniques relatives à ce service ou l'empêcherait de corriger une telle vulnérabilité ». Malgré les affirmations du gouvernement selon lesquelles il ne nuit pas au chiffrement, des lois similaires dans d'autres pays ont été utilisées pour miner le chiffrement, comme cela aurait été le cas avec Apple dans le régime britannique[17]. Cela ne devrait pas être permis au Canada.

La définition de la vulnérabilité systémique dans le projet de loi ne suffit pas pour limiter de façon importante le risque. La définition actuelle concerne uniquement l'accès non autorisé à des tiers, et ne concerne pas l'intégrité et la disponibilité des données, ou limite les vulnérabilités liées à un appareil, à un logiciel ou à un système d'exploitation. Les « vulnérabilités systémiques » doivent indiquer clairement qu'une obligation de miner ou de contourner le chiffrement est interdite, et il doit être clair que les vulnérabilités ne sont pas seulement liées à un accès non autorisé et ne sont pas seulement liées aux « services ». Plus précisément, l'ABC propose la définition suivante de « vulnérabilité systémique » :

> ***vulnérabilité systémique*** Désigne une vulnérabilité dans les protections électroniques qui crée un risque important pour la confidentialité, l'intégrité ou la disponibilité des renseignements, des services ou des systèmes.

17 *The Guardian*, « UK government resumes row with Apple by demanding access to British users' data » (1er octobre 2025) en ligne.

Modifier les paragraphes 5(5) et 7(5) pour exclure clairement le chiffrement :

> (5) Le [fournisseur principal/fournisseur de services électroniques] n'est pas tenu de se conformer à la disposition [d'un règlement pris en vertu du paragraphe (2)/d'une ordonnance] à l'égard d'un service ***électronique***, si le fait de s'y conformer l'obligerait à introduire une vulnérabilité systémique liée à ce service ou l'empêcherait de corriger une telle vulnérabilité, ou exigerait du fournisseur qu'il supprime, contourne ou nuise au chiffrement des renseignements.

F. Le gouvernement devrait accepter le risque qu'il propose de créer

En imposant des portes dérobées et en élargissant la conservation des données, la *Loi sur le soutien en matière d'accès autorisé à de l'information* créerait des cibles intéressantes pour les acteurs malveillants. La *Communications Assistance to Law Enforcement Act* aux États-Unis exigeait des portes dérobées similaires utilisées par des pirates informatiques étrangers pour obtenir des données des États-Unis[18]. Le Canada s'expose au même risque s'il impose des exigences similaires.

La conservation des métadonnées entre en conflit avec les lois canadiennes en matière de protection de la vie privée, qui limitent la conservation aux fins commerciales nécessaires et raisonnables. Les métadonnées en vertu de la *Loi sur le soutien en matière d'accès autorisé à de l'information* n'ont aucune finalité commerciale, ce qui risque d'entraîner des violations des lois sur la protection de la vie privée et les pratiques exemplaires et d'attirer les cybercriminels.

Dans l'ensemble, le régime devrait préciser les facteurs, les coûts admissibles et les directives pour le calcul de l'indemnité. De nombreuses dépenses en immobilisations des fournisseurs de services électroniques relevant de la partie 2 ne serviront à aucune fin commerciale et serviront uniquement à un accès légal. Si ces coûts profitent à la société, ils devraient être couverts par les recettes du gouvernement au lieu d'être imposés à certains fournisseurs de services électroniques. De plus, la *Loi sur le soutien en matière d'accès autorisé à de l'information* devrait indemniser les fournisseurs de services électroniques et les personnes touchées pour les pertes associées à la conformité, y compris les atteintes à la sécurité des données découlant des portes dérobées imposées par le gouvernement.

---

18 *Wall Street Journal*, « U.S. Wiretap Systems Targeted in China-Linked Hack: AT&T and Verizon are among the broadband providers that were breached » (5 octobre 2024) en ligne.

G. Obligation de prêter assistance

L'article 14 accorde à de nombreuses personnes chargées de la sécurité nationale le pouvoir de demander des renseignements aux fournisseurs de services électroniques. Il est excessif de permettre à quiconque – une personne civile ou autre – au sein d'organismes comme la GRC et le SCRS de demander des renseignements en vertu de la partie 2. La portée et les types de renseignements qui peuvent être demandés dans le cadre d'une telle obligation de communication doivent être restreints.

H. Contrôle judiciaire

Les articles 16 et 17 sont dépourvus d'imputabilité et de règle de droit. L'article 16 réduit au minimum le droit des fournisseurs de services électroniques de contester des ordonnances en instaurant l'obligation de fournir un préavis de 15 jours concernant une demande de contrôle judiciaire qui sera jointe à une lettre officielle adressée au ministre. L'article 16 ne contient aucun droit clair de contester le gouvernement.

I. Confidentialité obligatoire

La confidentialité énoncée à l'article 15 de la *Loi sur le soutien en matière d'accès autorisé à de l'information* est trop large et sans fondement. Il est interdit à tout fournisseur de services électroniques visé par un arrêté ministériel de divulguer à quiconque l'existence d'une telle ordonnance. Les entreprises doivent faire preuve de transparence au sujet de leurs produits, à moins qu'il n'y ait un impératif clair en matière d'application de la loi ou de sécurité nationale.

L'expérience au Royaume-Uni démontre qu'une loi similaire impose discrètement à Apple de supprimer le chiffrement de certains de ses produits principaux ou clés. Les entreprises américaines devraient pouvoir demander l'aide du gouvernement américain pour régler les ordonnances problématiques. Le ministre devrait justifier, au moyen d'un arrêté, la nécessité d'interdire la divulgation associée à ces ordonnances, et toute exigence de confidentialité devrait devenir caduque. Ces ordonnances devraient faire l'objet d'un contrôle judiciaire, et le ministre aurait le fardeau de convaincre le tribunal que l'interdiction de divulguer est raisonnablement nécessaire pour protéger la sécurité publique ou la sécurité nationale. Les entreprises non canadiennes, en particulier celles d'un pays du Groupe des cinq, doivent divulguer les ordonnances aux homologues de leur pays d'origine.

L'article 18 suggère d'autres règles en matière de confidentialité qui pourraient restreindre l'échange de renseignements, ce qui pourrait avoir une incidence sur les programmes d'attestation de sécurité des fournisseurs de services électroniques. La portée excessive prévue par le gouvernement dans ces articles est déraisonnable et indique un contrôle réglementaire excessif. Le contrôle judiciaire ne devrait donc pas être interdit. Le préavis et l'article 17, qui ajoute de l'ambiguïté pour limiter la divulgation des demandes d'accès, devraient être supprimés.

J. Pouvoirs d'inspection

Les articles 19 à 21 reprennent les pouvoirs d'enquête intrusifs de la *Loi sur la protection des cybersystèmes essentiels* (projet de loi C-8) conférant au ministre et aux personnes désignées des pouvoirs d'accès, qu'il s'agisse d'« examiner tout » ce qui se trouve sur les lieux ou d'emporter « tout ou partie d'un document, d'un registre ou d'un cybersystème » à des fins d'examen ou pour en faire des copies[19].

Ces pouvoirs – et articles – permettent de mener des enquêtes sans mandat pour les fournisseurs de services électroniques, autorisant l'examen et la reproduction de documents, avec l'obligation de prêter assistance. Il faudrait établir un seuil de motifs raisonnables et probables avant l'accès, afin d'établir un équilibre entre les vastes pouvoirs et l'absence de responsabilité pendant les enquêtes. Les inspections devraient a) exiger l'envoi d'un avis aux fournisseurs de services électroniques, b) être effectuées pendant les heures ouvrables normales, c) imposer aux inspecteurs de respecter les exigences raisonnables en matière de sécurité et de service des fournisseurs de services électroniques d) être effectuées de manière à réduire au minimum les répercussions sur les activités des fournisseurs de services électroniques.

K. Vérifications (article 21)

Pour vérifier le respect de la *Loi sur le soutien en matière d'accès autorisé à de l'information*, la personne désignée peut ordonner une vérification interne par les fournisseurs de services électroniques. Le fournisseur de services électroniques doit se conformer sans surveillance ou examen indépendants et sans garantie de confidentialité relativement au rapport subséquent, y compris les renseignements personnels qu'il contient. Les sections de l'ABC estiment que d'autres garanties procédurales sont nécessaires pour ce pouvoir de vérification, y compris un examen indépendant de l'ordonnance de vérification et du traitement de l'information.

---

19 Voir, par exemple, *Loi sur la protection des cybersystèmes essentiels*, paragraphes 49-50.

VI. RECOMMANDATIONS ANTÉRIEURES DE L'ABC

A. Codifier les principes de limitation de la finalité et de minimisation des données

Les sections de l'ABC recommandent que toute utilisation des renseignements recueillis par les organismes d'application de la loi ou les autorités de sécurité nationale se limite aux fins précises définies par la loi pour lesquelles ils ont été recueillis, avec des interdictions explicites de toute utilisation secondaire au-delà de l'autorisation initiale. Par exemple, les données informatiques conservées par le gouvernement en vertu de la partie 1 du projet de loi ne devraient pas être utilisées à d'autres fins que pour faire avancer l'enquête pour laquelle les données ont été saisies initialement. La collecte et la conservation des données doivent être proportionnelles et nécessaires à l'atteinte d'un objectif légitime du gouvernement[20].

B. Assurer l'uniformité entre les lois avec celles sur la protection de la vie privée

La nouvelle Loi ne devrait pas remplacer les droits à la protection de la vie privée ou les mécanismes de responsabilisation dans d'autres lois. Les sections de l'ABC recommandent un libellé affirmant que les mesures de protection de la vie privée existantes en vertu des lois fédérales et provinciales demeurent pleinement applicables[21].

C. Mandat de surveillance et de production de rapports indépendants

L'ABC appuie les obligations annuelles en matière de production de rapports publics au Parlement et un mécanisme de surveillance comme le commissaire à la protection de la vie privée, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement ou un autre tribunal désigné pour vérifier la conformité, examiner les plaintes et enquêter sur les cas d'abus ou de mauvaise utilisation.

D. Exiger un processus réglementaire transparent

La Loi accorde des pouvoirs importants aux futurs règlements. Par conséquent, les sections de l'ABC recommandent de mener des consultations auprès du public et des intervenants, en particulier les organismes de protection de la vie privée, les organismes juridiques et les organismes pour la défense des libertés civiques.

---

20 Référence : *OBA Submission on Privacy Guidance on facial Recognition for Police Agencies* (15 octobre 2021)

21 Résolution 15-04-M de l'ABC : Surveillance indépendante de l'Agence des services frontaliers du Canada (21 et 22 février 2015); présentation de l'ABC sur la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) (janvier 2017)

VII. CONCLUSION

Le projet de loi C-22 a des répercussions importantes qui touchent les intérêts des Canadiens en matière de protection de la vie privée, de sécurité et de cybersécurité. Les recommandations proposées par l'ABC se veulent une contribution de bonne foi aux délibérations importantes du Parlement dans l'élaboration de lois efficaces, compréhensibles et conformes à la *Charte*.