Projet de loi C-22, Loi concernant l'accès légal

Mémoire présenté au Comité permanent de la sécurité publique et nationale (SECU)

Coalition pour la surveillance internationale des libertés civiles

Présenté le 24 mai 2026

Introduction

La Coalition pour la surveillance internationale des libertés civiles (CSILC) est un regroupement d'organisations canadiennes fondé en 2002, au lendemain de l'adoption de la toute première *Loi antiterroriste* du Canada. Notre mandat est de surveiller les répercussions des lois canadiennes en matière de sécurité nationale et de lutte contre le terrorisme sur les libertés civiles, au Canada comme à l'étranger, et d'en défendre le respect. Les 45 organisations membres de la CSILC sont issues d'un large éventail de secteurs : groupes confessionnels, syndicaux, de défense des droits de la personne, environnementaux, juridiques et humanitaires.

Au cours des deux dernières décennies, nous avons observé avec inquiétude l'élargissement rapide des outils et des réseaux de surveillance gouvernementale, souvent assortis de garanties insuffisantes, en plus d'une érosion progressive des protections en matière de vie privée. Il s'agit notamment de la collecte et de la conservation de données sur les voyageurs (renseignements préalables sur les voyageurs et données des dossiers passagers), de l'octroi au Centre de la sécurité des télécommunications de vastes pouvoirs de surveillance, du recours par les forces de l'ordre – des corps de police locaux à la GRC – à des outils intrusifs comme les simulateurs de sites cellulaires et les outils de reconnaissance faciale (notamment ClearviewAI), d'investissements de plusieurs millions de dollars dans de nouveaux drones et tours de surveillance aux frontières canadiennes, et de la capacité accordée au Service canadien du renseignement de sécurité (SCRS) de recueillir des ensembles complets de données sans lien avec des menaces. De récents reportages ont par ailleurs mis en lumière le fait que les organismes d'application de la loi et de renseignement surveillent les mouvements autochtones et environnementaux sans justification depuis de nombreuses années[1].

Notre coalition a contribué de façon constante à ces débats, par des articles d'opinion, des mémoires, des soumissions dans le cadre de consultations et des comparutions devant des comités[2].

Maintes fois, des gouvernements fédéraux de toutes allégeances ont tenté d'affaiblir les protections en matière de vie privée au nom de l'« accès légal » – ce que d'autres ont justement qualifié de « loi zombie » qui revient sans cesse d'entre les morts. C'est le cas notamment du défunt projet de loi C-30, des propositions formulées dans le cadre de la consultation sur le Livre vert sur la sécurité nationale de 2016, de la Consultation de 2023 sur la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, et, en dernier lieu, du projet de loi C-2, Loi visant une sécurité rigoureuse à la frontière, aujourd'hui mis de côté. À chaque tentative, les gouvernements ont cherché à éroder considérablement les protections en matière de vie privée sous prétexte de doter la police et le SCRS de pouvoirs pour lutter contre les activités illicites – qu'il s'agisse du terrorisme, du recyclage des produits

[1] Brodie Fenlon, « How the RCMP spied on Indigenous organizations — and how we broke the story », *CBC News*, 24 mars 2026. En ligne : https://www.cbc.ca/news/editorsblog/cbc-news-indigenous-rcmp-surveillance-9.7133525

[2] Voir par exemple : https://iclmg.ca/atf-consultation/, https://iclmg.ca/opc-biometrics-consultation/, https://iclmg.ca/mr-paulson-we-have-enough-power-to-fight-cybercrime/, https://iclmg.ca/wp-content/uploads/2016/12/Nat-Sec-Consultation-ICLMGs-Answers-EN.pdf, https://iclmg.ca/issues/bill-c-59-the-national-security-act-of-2017/bill-c-59s-mass-surveillance-and-cyber-powers/

de la criminalité et du financement des activités terroristes, ou de l'exploitation en ligne. Cependant, chaque fois, il est devenu évident que la population canadienne refuse de troquer les protections importantes qu'offrent les lois sur la vie privée contre des promesses de « sécurité » fondées sur des justifications nébuleuses quant à la nécessité de ces pouvoirs pour les forces de l'ordre. On observe par ailleurs un schéma récurrent – notamment dans le cas du projet de loi C-22 – selon lequel, bien que la police et les forces de l'ordre fassent valoir que de nouveaux pouvoirs d'enquête sont nécessaires pour faire face à des défis inédits, les données probantes démontrent que les outils et les pouvoirs nécessaires pour y répondre adéquatement existent déjà. Comme l'a relevé le Citizen Lab, ce que les forces de l'ordre présentent comme un obstacle constitue en réalité de simples difficultés dans le déroulement des enquêtes, qui peuvent néanmoins être menées efficacement[3].

Même dans son récent rapport sur l'accès légal – qui est relativement favorable à l'adoption de nouvelles lois en la matière –, le Comité des parlementaires sur la sécurité nationale et le renseignement a conclu que les organismes d'application de la loi et de renseignement ne disposent pas des données probantes nécessaires pour démontrer la nécessité de ces nouveaux pouvoirs, et qu'ils ont été en grande partie efficaces sans les outils qu'ils réclament comme étant si urgents[4].

Position de la Coalition sur le projet de loi C-22

Notre coalition est profondément préoccupée par le fait que, s'il est adopté, le projet de loi C-22 renforcera la surveillance exercée par l'État et menacera sérieusement le droit à la vie privée, ce qui aura des répercussions simultanées sur la liberté d'expression, la liberté d'association et le droit à l'égalité. Un tel élargissement de la surveillance étatique porte également atteinte aux obligations internationales du Canada en matière de droits de la personne et de libertés civiles, notamment l'article 2 (non-discrimination), l'article 12 (vie privée), l'article 19 (liberté d'opinion et d'expression) et l'article 20 (liberté de réunion et d'association pacifiques) de la Déclaration universelle des droits de l'homme[5], ainsi que l'article 2.1 (non-discrimination), l'article 17 (vie privée), l'article 19 (liberté d'expression) et l'article 22 (association) du Pacte international relatif aux droits civils et politiques[6].

Cette loi constitue l'une des plus grandes menaces pour la vie privée au Canada depuis deux décennies. Ses dispositions affaibliront les règles régissant l'accès des forces de l'ordre aux renseignements personnels, tout en facilitant un vaste élargissement de la surveillance

[3] Christopher Parsons, « Canada's New and Irresponsible Encryption Policy », *The Citizen Lab*, 21 août 2019. En ligne : https://citizenlab.ca/research/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

[4] 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*, Sa Majesté le Roi du chef du Canada, 2025. En ligne : https://www.nsicop-cpsnr.ca/reports/rp-2025-09-15-sr/250915_CPSNR_Rapport_sur_l%E2%80%99acc%C3%A8s_l%C3%A9gal.pdf

[5] Nations Unies, *Déclaration universelle des droits de l'homme*, 10 décembre 1948. En ligne : https://www.un.org/fr/about-us/universal-declaration-of-human-rights

[6] Nations Unies (Assemblée générale), « Pacte international relatif aux droits civils et politiques », *Recueil des traités*, vol. 999, décembre 1966, p. 171. En ligne : https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

gouvernementale. Comme nous l'avons exposé ci-dessus, il s'agit une fois de plus d'une illustration manifeste de la tendance, observée depuis des décennies, des gouvernements à se servir de la sécurité nationale comme prétexte pour éroder les libertés civiles et les droits de la personne.

Le projet de loi C-22 est de portée plus limitée que son prédécesseur, le projet de loi C-2, puisqu'il porte exclusivement sur l'accès légal et contient certaines modifications visant à répondre aux critiques antérieures. Cependant, non seulement ces changements sont insuffisants, mais le gouvernement a ajouté au projet de loi C-22 une nouvelle disposition sur la conservation des données qui soulève d'importantes préoccupations supplémentaires en matière de vie privée.

Par ailleurs, comme l'a exposé en détail le professeur Michael Geist dans un article récent, le gouvernement a une fois de plus omis de présenter des données probantes ou des scénarios convaincants pour justifier les réformes législatives qu'il cherche à obtenir par cette loi[7].

Compte tenu de ces préoccupations, notre coalition demande aux députés de rejeter le projet de loi C-22 et de voter contre. Si le projet de loi devait néanmoins poursuivre son cheminement parlementaire, des amendements importants devraient à tout le moins être apportés à la partie 1, et la partie 2 devrait être retirée.

Partie 1 : Accès aux données et aux renseignements en temps opportun

a. « Ordre de fournir des renseignements » et « ordre de confirmer la fourniture de services »

La partie 1 du projet de loi C-22, *Accès aux données et aux renseignements en temps opportun*, a été modifiée par rapport au projet de loi C-2 sur un point important : elle restreint les vastes pouvoirs dont disposaient auparavant la police et les agents de renseignement en vertu du projet de loi C-2 pour obliger les entreprises offrant des services au public à fournir des renseignements sur les titulaires de comptes sans mandat, pouvoirs antérieurement désignés sous le nom d'« ordre de fournir des renseignements ».

De telles demandes seraient désormais limitées aux fournisseurs de services de télécommunication et aux simples réponses par oui ou par non quant à savoir si un fournisseur de services de télécommunication détient un compte associé au nom, à l'adresse courriel, au numéro de téléphone d'une personne, etc. Bien que plus restreint, le précédent que constitue le fait d'autoriser des agents à demander des renseignements sans mandat, fondé sur un simple soupçon – plutôt que d'une croyance – que les renseignements seraient utiles à une enquête criminelle demeure préoccupant, et soulève des inquiétudes quant à la possibilité que cette pratique soit élargie à l'avenir à mesure qu'elle se normalisera.

---

[7] Michael Geist, « The Government Tries to Make the Case for Bill C-22: Why Its Own Use Cases Reveal Disproportionate Overreach », *michaelgeist.ca*, 21 mai 2026. En ligne : https://www.michaelgeist.ca/2026/05/the-government-tries-to-make-the-case-for-bill-c-22-why-its-own-use-cases-reveal-disproportionate-overreach/ [*Geist*, 2026]

Malheureusement, d'autres problèmes graves que posait cette partie de la loi n'ont pas été réglés.

b. Ordonnances de communication visant les renseignements relatifs à l'abonné

Le projet de loi C-22 créera un nouveau pouvoir d'« ordonnance de communication » fondé sur le seuil très bas des « motifs raisonnables de soupçonner » permettant à la police d'obtenir des renseignements personnels sur les clients de toute entité offrant un service au public (désignés sous le nom de « renseignements relatifs à l'abonné »).

Bien que les « renseignements relatifs à l'abonné » aient été décrits comme étant de portée limitée, ils englobent en réalité des renseignements très vastes et révélateurs, notamment :

a. les renseignements permettant d'identifier l'abonné ou le client, notamment ses nom, pseudonyme, adresse, numéro de téléphone et adresse de courriel;
b. l'identifiant que la personne a attribué à l'abonné ou au client, notamment des numéros de compte;
c. les renseignements relatifs aux services fournis à l'abonné ou au client, notamment :
    i. les types de services fournis,
    ii. la période durant laquelle les services ont été fournis,
    iii. les renseignements qui identifient les dispositifs, équipements ou choses utilisés par l'abonné ou le client en lien avec les services.

De tels renseignements peuvent être très révélateurs des aspects personnels de la vie d'un individu, bien plus que de simples « renseignements d'annuaire ». Compte tenu de l'étendue des renseignements visés, le seuil des motifs raisonnables de soupçonner est nettement trop bas. À tout le moins, le seuil devrait demeurer celui des motifs raisonnables de croire – qui est la norme actuellement applicable pour demander ce type de renseignements à un fournisseur de services.

Le projet de loi C-22 créera en outre un nouveau pouvoir extraterritorial permettant aux forces de l'ordre de présenter une « demande » à des services de télécommunication étrangers pour obtenir les renseignements qu'ils détiennent – encore une fois fondé sur le même seuil minimal des « motifs raisonnables de soupçonner ».

c. Modifications apportées à la *Loi sur l'entraide juridique en matière criminelle*

Le projet de loi C-22 propose également de modifier la *Loi sur l'entraide juridique en matière criminelle* en créant un régime permettant à des entités étrangères de soumettre au ministre de la Justice une demande de communication de données de transmission ou de renseignements relatifs à l'abonné se trouvant en la possession ou à la disposition d'une personne au Canada. Ces demandes seraient ensuite soumises à un juge qui pourrait les autoriser. Comme pour la nouvelle ordonnance de communication visant les renseignements relatifs à l'abonné décrite ci-dessus, la demande n'a à satisfaire qu'au bas seuil des « motifs raisonnables de soupçonner ». Ce seuil est une fois de plus bien trop bas pour autoriser la

collecte de renseignements susceptibles de toucher à des intérêts importants en matière de vie privée.

Au-delà du seuil peu élevé, il n'existe aucune exigence de double incrimination – l'infraction étrangère n'a donc pas à constituer une infraction au Canada –, ce qui pose de sérieux risques que le système juridique canadien puisse soutenir des enquêtes portant sur des comportements qui ne seraient pas criminels ici. Cette préoccupation est aggravée par le fait qu'une fois les renseignements communiqués à une entité étrangère, ils échappent au contrôle juridique canadien et peuvent être utilisés ou partagés d'une manière qui contreviendrait au droit canadien ou à la *Charte canadienne des droits et libertés*.

Contrairement à d'autres formes de communication de renseignements entre ministères gouvernementaux et entités étrangères, qui peuvent être régies par la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, aucune mesure de protection n'est intégrée dans la loi pour évaluer les risques que les renseignements divulgués entraînent de graves mauvais traitements à l'égard d'une personne.

Enfin, il y a de sérieuses préoccupations quant au fait que ces modifications ouvriront la voie à la ratification par le Canada du Deuxième Protocole additionnel à la Convention de Budapest et à la négociation d'un accord avec les États-Unis dans le cadre de la CLOUD Act, l'un et l'autre présentant des menaces importantes pour la vie privée et d'autres droits de la personne. Pour une analyse plus approfondie, nous vous renvoyons au rapport du Citizen Lab intitulé *Unspoken Implications*[8], ainsi qu'au mémoire d'OpenMedia sur le projet de loi C-22[9].

Pour ces raisons, nous nous opposons à l'adoption de la partie 1 du projet de loi C-22.

Partie 2 : *Loi sur le soutien en matière d'accès autorisé à de l'information*

Ce qui préoccupe le plus dans le projet de loi C-22, c'est la création proposée de la *Loi sur le soutien en matière d'accès autorisé à de l'information*.

Par le biais de règlements publics et d'arrêtés secrets, la *Loi sur le soutien en matière d'accès autorisé à de l'information* permettrait au gouvernement d'obliger la vaste catégorie des « fournisseurs de services électroniques » à apporter des modifications étendues et radicales à leurs systèmes afin de faciliter l'accès des forces de l'ordre, ainsi qu'à conserver des données personnelles sensibles sur les utilisateurs pendant une période pouvant aller jusqu'à un an, sans mesures de protection adéquates contre les vulnérabilités de sécurité que de tels arrêtés créeront. Le nouveau régime serait également dépourvu de dispositions adéquates en matière de responsabilisation et de transparence.

---

[8] Kate Robertson, « Unspoken Implications », *The Citizen Lab*, 16 juin 2025. En ligne : https://citizenlab.ca/research/a-preliminary-analysis-of-bill-c-2/

[9] OpenMedia, *Projet de loi C-22, Loi concernant l'accès légal*, OpenMedia, 15 mai 2026. En ligne : https://www.ourcommons.ca/Content/Committee/451/SECU/Brief/BR14120373/br-external/OpenMedia-067260526073-f.pdf [*OpenMedia*, 2026]

Prises dans leur ensemble, les dispositions de la *Loi sur le soutien en matière d'accès autorisé à de l'information* constituent l'un des élargissements les plus importants de l'appareil de surveillance étatique des vingt dernières années. Si elles sont adoptées, elles menaceront non seulement le droit à la vie privée, mais aussi les libertés qui y sont associées, notamment la liberté d'expression, la liberté d'association et les droits à l'égalité. Elles contribuent en outre à consolider l'écosystème plus large d'arrêtés secrets, de processus décisionnels opaques et d'enquêtes secrètes qui caractérise le régime canadien de sécurité nationale et de lutte contre le terrorisme, et qui continue d'engendrer des abus de la part de la police et des services de renseignement, une surveillance et des enquêtes injustifiées à l'égard des communautés racialisées et autochtones, ainsi que des violations des obligations nationales et internationales du Canada en matière de droits de la personne et de libertés civiles.

Enfin, les dispositions de la *Loi sur le soutien en matière d'accès autorisé à de l'information* sont en grande partie inchangées par rapport à ce qui avait été présenté dans le projet de loi C-2. De nouvelles mesures de protection ont certes été introduites, mais celles-ci sont contrebalancées par, entre autres, l'escalade des pouvoirs d'émission d'arrêtés pour inclure la conservation des métadonnées pendant un an.

Bien que le gouvernement affirme avoir tenu compte des préoccupations des experts en matière de protection de la vie privée, de libertés civiles et de sécurité nationale, cela n'est vrai que pour la partie 1. Malgré des mises en garde répétées quant aux lacunes fondamentales de la *Loi sur le soutien en matière d'accès autorisé à de l'information*, le gouvernement est revenu avec essentiellement le même cadre.

Compte tenu de tout cela, la CSILC se joint à d'autres pour recommander que la partie 2 du projet de loi C-22 soit retirée, et exhorte les membres du Comité et tous les parlementaires à voter contre.

Problème 1 : Le champ d'application de la *Loi sur le soutien en matière d'accès autorisé à de l'information* est excessivement large

Les pouvoirs de prise de règlements et d'arrêtés prévus par la *Loi sur le soutien en matière d'accès autorisé à de l'information* s'appliqueront à tous les « fournisseurs de services électroniques ». Bien que le public puisse supposer que cette catégorie vise les fournisseurs de services de télécommunication et d'accès à Internet, ou les grands sites de médias sociaux et de communications numériques, sa portée est bien plus large. Un fournisseur de services électroniques est défini comme une « [p]ersonne qui, seule ou au titre de son appartenance à un groupe, fournit des services électroniques, notamment en vue de permettre la communication, et qui, selon le cas : a) fournit ces services à des personnes se trouvant au Canada; b) exerce tout ou partie de ses activités commerciales au Canada ».

Un « service électronique » est en outre défini comme « [t]out service – ou fonctionnalité d'un service – qui implique la création, l'enregistrement, le stockage, le traitement, la transmission, la réception, la diffusion ou la mise à disposition d'information sous toute forme immatérielle, notamment électronique ou numérique, par tout moyen technologique – électronique,

numérique, magnétique, optique, biométrique, acoustique ou autre – ou par une combinaison de tels moyens ».

Si cette catégorie englobe les grandes plateformes en ligne et les entreprises de télécommunication telles que Meta, X, Amazon, Bell et Rogers, elle va bien au-delà. Elle pourrait également viser les librairies locales, les fournisseurs de services de santé mentale, les institutions financières, les sites de réservation de voyages, les sites de rencontres et bien d'autres – essentiellement toute entité permettant aux utilisateurs de créer des comptes, de communiquer ou de prendre des rendez-vous en ligne. Certains se sont même demandé si les exploitants de sites Web ou de blogues permettant l'échange de messages pourraient être visés. Il s'agit d'une catégorie d'une ampleur inacceptable, et le gouvernement n'a pas expliqué pourquoi il est nécessaire de viser un éventail aussi vaste d'entreprises.

Les fournisseurs de services électroniques seront répartis en deux catégories : les fournisseurs principaux et tous les autres fournisseurs de services électroniques. Toutefois, les fournisseurs principaux ne seront définis par règlement qu'après l'entrée en vigueur de la *Loi sur le soutien en matière d'accès autorisé à de l'information*, de sorte qu'il est impossible de savoir avec certitude quels fournisseurs de services électroniques relèveront de cette catégorie.

Le gouverneur en conseil peut prendre des règlements publics régissant les catégories de fournisseurs principaux. Bien que la divulgation publique soit un aspect positif, elle est compromise par le pouvoir du ministre de la Sécurité publique d'émettre des arrêtés ministériels à l'égard de tous les fournisseurs de services électroniques, y compris les fournisseurs principaux. La véritable portée des arrêtés imposés aux principaux fournisseurs de services électroniques sera donc impossible à connaître, et rien ne sera connu des arrêtés imposés à tous les autres fournisseurs de services électroniques. Bien que des mesures de protection existent – notamment l'obligation pour le commissaire au renseignement d'approuver les arrêtés ministériels avant leur entrée en vigueur –, comme il est expliqué ci-dessous, elles ne vont pas assez loin.

Problème 2 : Les pouvoirs d'émission d'arrêtés sont excessivement larges

Les règlements publics et les arrêtés ministériels autorisés en vertu de la *Loi sur le soutien en matière d'accès autorisé à de l'information* peuvent être utilisés aux mêmes fins.

Ces fins comprennent les suivantes :

- l'élaboration, la mise en œuvre […] et le maintien [des] capacités opérationnelles et techniques, notamment en ce qui touche l'extraction et l'organisation de l'information […] et l'accès à celle-ci;
- l'installation, l'utilisation, le fonctionnement […] et l'entretien de tout dispositif ou équipement ou de toute autre chose pouvant permettre à la personne autorisée d'accéder à de l'information.

Ces deux dispositions figuraient déjà dans le projet de loi C-2. Cependant, le gouvernement a ajouté une nouvelle disposition profondément préoccupante : la conservation de catégories de

métadonnées pendant une période pouvant aller jusqu'à un an. Ces pouvoirs sont exceptionnellement larges, même pour des règlements publics, et a fortiori pour des arrêtés ministériels secrets. Ils pourraient être utilisés de façons difficiles à prévoir, avec des conséquences – intentionnelles et non intentionnelles – qu'il est impossible d'anticiper pleinement.

Parmi les scénarios que l'on peut envisager aujourd'hui :

- Le gouvernement pourrait, publiquement ou secrètement, ordonner aux fournisseurs de services électroniques de modifier leurs systèmes afin de permettre la surveillance en temps réel des communications, la collecte et la conservation de renseignements sur les communications par les forces de l'ordre ou le SCRS, ou de toute autre manière faciliter l'accès aux données.
    - Par exemple : pouvoir recueillir des renseignements en temps réel sur le réseau d'un fournisseur de services Internet.
    - Par exemple : créer des portes dérobées dans des dispositifs de messagerie privée, voire dans des messageries chiffrées.
- Le gouvernement pourrait ordonner aux fournisseurs de services électroniques d'organiser les renseignements qu'ils recueillent déjà de manière à les rendre plus accessibles et utiles pour les forces de l'ordre ou le SCRS, notamment dans le cadre de la collecte d'ensembles de données du SCRS.
- Le gouvernement pourrait ordonner aux fournisseurs de services électroniques de recueillir des métadonnées très révélatrices – des données sur nos communications, notamment les expéditeurs, les destinataires, l'heure, la date, le lieu et nos activités – pendant une période pouvant aller jusqu'à un an, sans lien avec une enquête.

Quels sont les risques?

- Élargissement rapide des pouvoirs de surveillance étatique. Nous avons vu dans le passé comment les nouveaux pouvoirs de surveillance, en particulier ceux exercés en secret, tendent à s'élargir avec le temps, entraînant des violations de droits, une surveillance illégale et des atteintes aux droits.
- Les portes dérobées et les systèmes de surveillance, une fois en place, ne se limitent pas à l'usage des organismes d'application de la loi et de renseignement canadiens, ni à celui des alliés du Canada :
    - Ils peuvent également être accessibles et exploités par tout organisme étranger d'application de la loi ou de renseignement.
    - Ils peuvent faire l'objet d'attaques, de piratage, de fuites ou d'utilisations abusives.
    - L'attaque « Salt Typhoon » de 2023-2024 constitue un exemple crucial : elle a exploité des portes dérobées et des points d'accès pour faciliter les capacités d'interception en matière de sécurité nationale aux États-Unis.

Deux domaines de risque sont particulièrement préoccupants :

Premièrement, comme il est expliqué dans la section suivante, les mesures de protection proposées contre les « vulnérabilités systémiques » sont bien trop insuffisantes. Combinées à

l'étendue du champ d'application de ce que l'on peut ordonner aux fournisseurs de services électroniques de faire, elles se traduiront par un affaiblissement général des communications privées et de la transmission de données en ligne. Cela est particulièrement vrai en raison de l'absence de protections spécifiques et claires pour les données chiffrées. Les dispositions de la loi laissent ouverte la possibilité que, sous l'actuel gouvernement ou un gouvernement futur, des portes dérobées soient intégrées dans les communications chiffrées. Même si ces portes dérobées ne correspondent pas aux clés de chiffrement elles-mêmes, elles n'en constitueront pas moins des vulnérabilités susceptibles de rendre illusoires les protections offertes par le chiffrement. La protection de nos renseignements personnels et de nos communications en ligne est fondamentale pour pouvoir exercer tous les droits et libertés civiles qui y sont associés dans un écosystème devenu essentiel à nos activités quotidiennes. Le projet de loi C-22 constitue une menace manifeste pour ces protections.

Deuxièmement, la nouvelle disposition sur la conservation des métadonnées est inacceptable. Elle soulève de graves préoccupations quant à la transformation des entreprises privées en agents de collecte de données pour le gouvernement. Les métadonnées ne contiennent peut-être pas le contenu des communications, mais ce qu'elles dévoilent sur la vie privée est extrêmement révélateur – avec qui nous parlons, où nous nous déplaçons, quand nous nous livrons à certaines activités. Elles peuvent également exposer des réseaux entiers d'association en établissant des liens entre les personnes qui se parlent, qui voyagent aux mêmes endroits aux mêmes moments, et ainsi de suite. L'obligation de conserver de telles données personnelles engage donc l'article 8 de la *Charte canadienne des droits et libertés*, qui protège contre les fouilles, perquisitions et saisies abusives. Comme l'a fait remarquer le professeur Michael Geist, le résultat serait « une carte de surveillance de pratiquement chaque Canadien[10] ». En aucun cas une telle quantité de renseignements personnels ne devrait être ordonnée conservée sans autorisation judiciaire. Même dans ce cas, l'autorisation de conserver des données pendant une année complète devrait être traitée comme une circonstance exceptionnelle assortie d'exigences probatoires élevées.

Au-delà des implications pour la *Charte*, cette disposition a également des répercussions importantes sur la sécurité des données. Un tel volume de données constituerait une véritable mine d'or pour les pirates informatiques, les entités étrangères et d'autres acteurs malveillants. Il serait également propice aux abus de la part d'employés des entreprises qui collectent les données ou des forces de l'ordre qui y ont accès – comme en témoignent de nombreux cas documentés d'agents ayant détourné des bases de données existantes pour surveiller d'ex-partenaires ou des personnes qu'ils trouvaient attrayantes.

Enfin, la pleine mesure de la façon dont ces renseignements pourraient être utilisés par les organismes d'application de la loi et de renseignement, tant nationaux qu'étrangers, n'a pas été rendue manifeste par les exemples fournis par le gouvernement. Les scénarios présentés portent notamment sur la localisation de téléphones utilisés par de présumés terroristes, la possibilité de retracer et de secourir des enfants kidnappés en toute sécurité, ou encore la lutte contre des individus anonymes se livrant à l'exploitation sexuelle de mineurs. Cependant, les utilisations potentielles vont bien au-delà :

[10] *Geist,* 2026 [TRADUCTION].

- Ces données sur la localisation et les communications offriraient encore plus de possibilités de surveillance et de pistage des défenseurs autochtones des terres ou d'autres militants, comme l'a récemment révélé *CBC*. De futurs gouvernements pourraient s'en servir pour cibler tout sous-groupe de la population qu'ils considèrent comme une menace pour leurs politiques (indépendamment de toute menace réelle de violence).
- Ces données pourraient également être utilisées pour un pistage à l'américaine des immigrants et des réfugiés afin d'accélérer les expulsions.
- La collecte et l'organisation de métadonnées, sur des Canadiens et des personnes étrangères, constitueraient une aubaine pour les pouvoirs de collecte d'ensembles de données du SCRS, déjà critiqués par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) pour avoir fonctionné de manière inédite et sans reddition de comptes depuis leur adoption en 2019.
- Des organismes étrangers d'application de la loi, notamment les États-Unis, pourraient y accéder à des fins d'enquêtes et de poursuites menaçant des communautés entières – notamment les personnes cherchant à avorter ou à obtenir d'autres soins de santé reproductive, ou des soins d'affirmation de genre (y compris des citoyens américains accédant légalement à ces soins au Canada).

Problème 3 : Mesures de protection insuffisantes et secret injustifié

Bien que la *Loi sur le soutien en matière d'accès autorisé à de l'information* prévoie des mesures de protection, celles-ci sont nettement insuffisantes.

Premièrement, la portée des conditions de non-divulgation est inacceptable. Les arrêtés ministériels secrets peuvent couvrir l'ensemble des modifications apportées aux systèmes des fournisseurs de services électroniques – des plus anodines aux plus importantes; il est prévisible que ce seront les arrêtés les plus sensibles et les plus controversés qui seront émis en secret. Les fournisseurs de services électroniques seront soumis à une obligation de non-divulgation indéfinie, non seulement quant au contenu d'un arrêté, mais même quant au fait d'en avoir reçu un. Rien ne justifie ce niveau de secret pour l'ensemble des arrêtés émis à l'égard de fournisseurs de services électroniques individuels.

La portée et les répercussions des arrêtés ministériels secrets méritent un contrôle judiciaire, et non le seul examen du commissaire au renseignement. Bien que le commissaire au renseignement soit un juge à la retraite agissant en toute indépendance, le poste est susceptible d'être politisé ou de faire l'objet de compressions budgétaires. Seul un contrôle judiciaire offrirait la certitude nécessaire – si tant est que les arrêtés secrets soient acceptables.

Ces préoccupations ne sont pas davantage dissipées par les rapports publics ni par l'examen obligatoire prévu trois ans après l'entrée en vigueur du régime de la *Loi sur le soutien en matière d'accès autorisé à de l'information*.

Au cœur de ces préoccupations se trouve le fait que ce nouveau régime contribuera à élargir encore davantage le nombre croissant d'arrêtés, de procédures et de régimes secrets sous

couvert de protection de la sécurité nationale. Cela comprend le recours aux procès secrets pour les certificats de sécurité, les processus administratifs à huis clos qui sous-tendent le Programme de protection des passagers et la liste des entités terroristes, les pouvoirs de réduction de la menace du SCRS, ainsi que d'autres pouvoirs élargis accordés en vertu de la *Loi concernant la lutte contre l'ingérence étrangère*, et les opérations cybernétiques actives et défensives du Centre de la sécurité des télécommunications, entre autres. Tout cela est étayé par le recours croissant à la preuve secrète devant les tribunaux. Cette preuve secrète est utilisée en grande partie pour éviter de révéler les méthodes d'enquête employées par les forces de l'ordre et le SCRS; un nouveau régime destiné à élargir considérablement la capacité de ces organismes à mener des actions d'enquête secrètes ne fera qu'aggraver ce problème.

Nous nous associons également à la préoccupation de l'OSSNR, qui juge incompréhensible que l'organisme n'ait pas reçu un rôle plus important dans ce régime. Comme l'a suggéré l'OSSNR, il devrait à tout le moins recevoir les rapports et les renseignements sous-jacents afin de faciliter un examen proactif à l'avenir.

Les mesures de protection proposées contre les vulnérabilités systémiques sont également tout à fait insuffisantes.

Premièrement, comme l'expose en détail OpenMedia dans son mémoire[11], la structure même de la *Loi sur le soutien en matière d'accès autorisé à de l'information* compromet ces protections de deux façons : d'abord, en accordant au gouvernement le pouvoir de redéfinir tout terme de la loi par simple règlement; ensuite, en disposant à la fois qu'un fournisseur de services électroniques n'est pas tenu de donner suite à un arrêté qui créerait une vulnérabilité systémique, mais aussi qu'il commet une infraction s'il n'exécute pas un arrêté.

Même si ces problèmes législatifs étaient résolus, la définition de vulnérabilité systémique est profondément déficiente. La *Loi sur le soutien en matière d'accès autorisé à de l'information* définit une vulnérabilité systémique comme :

> Toute vulnérabilité dans les protections électroniques d'un service électronique qui crée un risque sérieux **qu'une personne puisse accéder à de l'information sécurisée sans en avoir le droit ou l'autorisation**. [GRAS AJOUTÉ]

Cette protection repose sur l'idée qu'il serait possible de créer une vulnérabilité qui ne pourrait pas, avec un degré élevé de certitude, être exploitée par une personne non autorisée. Or, premièrement, le « risque sérieux » est une notion subjective, qui laisse ouverte la réelle possibilité que la tentation de créer des vulnérabilités utiles à la sécurité nationale ou aux forces de l'ordre érode graduellement ce seuil. Deuxièmement, comme le démontre l'exemple de Salt Typhoon et les récentes expériences en matière d'intelligence artificielle, il est extrêmement difficile – voire impossible – d'évaluer le risque que présentent les vulnérabilités une fois en place. Fonder une protection clé sur l'hypothèse que seuls le Canada et ses alliés auront accès à ces points d'entrée fait peser un risque sérieux sur la sécurité de nos communications en ligne.

[11] *OpenMedia*, 2026.

Conclusion

En réponse au projet de loi C-2, des centaines d'organisations de la société civile ont dénoncé les graves atteintes qu'il portait aux droits fondamentaux au Canada. Au cœur de ces préoccupations se trouvaient les nouveaux pouvoirs de surveillance. Bien que le projet de loi C-22 fasse des efforts modestes pour y répondre, il continue de proposer des modifications législatives qui constituent non seulement une menace pour le droit à la vie privée, mais aussi pour un large éventail de droits connexes qui dépendent de l'accès à des communications privées exemptes de toute surveillance et ingérence gouvernementale injustifiée. Le projet de loi C-22 crée également, sans justification, des risques pour la cybersécurité qui menaceront davantage les renseignements personnels non seulement des personnes au Canada, mais aussi de tous les individus dont les données sont détenues par des fournisseurs de services électroniques assujettis au nouveau régime de règlements et d'arrêtés ministériels secrets créé par la *Loi sur le soutien en matière d'accès autorisé à de l'information*.

Compte tenu de ces préoccupations, notre coalition demande aux députés de rejeter le projet de loi C-22 et de voter contre. Si le projet de loi C-22 devait néanmoins poursuivre son cheminement parlementaire, des amendements importants devraient à tout le moins être apportés à la partie 1, et la partie 2 devrait être retirée.