

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

Mémoire présenté au Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants

Coalition pour la surveillance internationale des libertés civiles

Présenté le 4 novembre 2026

À propos de la Coalition pour la surveillance internationale des libertés civiles
La Coalition pour la surveillance internationale des libertés civiles est une coalition d'organisations canadiennes fondée en 2002 à la suite de l'adoption de la toute première *Loi antiterroriste* du Canada. Notre mandat est de surveiller les répercussions des lois canadiennes sur la sécurité nationale et l'antiterrorisme sur les libertés civiles au Canada et à l'international, et de nous en défendre. Les 45 organismes membres de la coalition couvrent un large éventail de secteurs, notamment des organismes confessionnels, syndicaux, environnementaux, juridiques et humanitaires et de défense des droits de la personne. Pour en savoir plus : http://iclmg.ca [EN ANGLAIS].

Introduction

Au cours des deux dernières décennies, les gouvernements fédéraux successifs ont tenté d'affaiblir les protections de la vie privée au nom de l'« accès légal ». Chaque fois, toutefois, les spécialistes de la protection de la vie privée, les défenseurs et défenseuses des droits de la personne et des libertés civiles ainsi que la population en général ont refusé de sacrifier les importantes protections que nous offrent les lois sur la protection de la vie privée en échange de promesses de « sécurité » fondées sur des justifications nébuleuses voulant que ces pouvoirs soient nécessaires aux forces de l'ordre. Notre coalition a régulièrement pris part à ces débats au moyen de lettres d'opinion, de mémoires, de contributions aux consultations et de comparutions devant des comités[1].

On observe aussi une tendance récurrente, y compris dans le cas du projet de loi C-22 : les forces de l'ordre soutiennent que de nouveaux pouvoirs d'enquête leur sont indispensables pour relever des défis inédits, alors que les données probantes montrent qu'elles disposent déjà d'outils et de pouvoirs qui leur permettraient de régler adéquatement ces problèmes. Comme l'explique le Citizen Lab, les forces de l'ordre présentent parfois ces problèmes comme un blocage, mais elles se heurtent en réalité à des frictions d'enquête : les difficultés existent, mais les enquêtes peuvent quand même être menées efficacement[2]. De plus, comme l'a exposé en détail le professeur Michael Geist, le gouvernement n'a, encore une fois, présenté aucun élément de preuve ni aucun scénario convaincant pour justifier les réformes qu'il cherche à faire adopter au moyen de ce projet de loi[3].

[1] Voir, par exemple : https://iclmg.ca/atf-consultation/, https://iclmg.ca/opc-biometrics-consultation/, 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/ [EN ANGLAIS].
[2] Christopher Parsons, *Canada's New and Irresponsible Encryption Policy*, The Citizen Lab, 21 août 2019.
[3] 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.

Position sur le projet de loi C-22

Notre coalition craint vivement que le projet de loi C-22, s'il est adopté, n'élargisse considérablement la surveillance étatique et ne menace gravement le droit à la vie privée, avec des répercussions concomitantes sur la liberté d'expression, la liberté d'association et les droits à l'égalité.

Ce projet de loi représente l'une des plus graves menaces pour la vie privée au Canada des deux dernières décennies. Ses dispositions affaibliront les règles qui encadrent l'accès de la police aux renseignements personnels, tout en facilitant une vaste expansion de la surveillance gouvernementale, et créeront une mine de données qui attirera irrésistiblement les pirates informatiques. Il s'inscrit dans la tendance, observée depuis des décennies, des gouvernements canadiens à invoquer la sécurité nationale pour justifier l'érosion des libertés civiles et des droits de la personne.

Nous reconnaissons que la Chambre des communes a adopté plusieurs amendements pour répondre aux préoccupations que nous et d'autres avons soulevées, mais, pour les raisons exposées ci-dessous, nous estimons que ces amendements ne règlent pas les problèmes de fond du projet de loi C-22.

Recommandation 1 : Compte tenu des préoccupations exposées ci-dessous, le projet de loi C-22 ne devrait pas recevoir la sanction royale; il devrait plutôt être retiré, réexaminé et soumis à de plus amples consultations. Subsidiairement, les préoccupations non résolues concernant la partie 1 du projet de loi devraient être réglées au moyen d'amendements ciblés, et la partie 2 devrait être entièrement retirée.

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

a. « Ordres 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*, prévoit un nouvel « ordre de confirmer la fourniture de services ». Cet ordre viserait uniquement les fournisseurs de services de télécommunication et se limiterait à une réponse par oui ou par non indiquant si le fournisseur détient un compte associé au nom, à l'adresse courriel, au numéro de téléphone, etc., d'une personne.

Malgré leur portée restreinte, les « ordres de confirmer la fourniture de services » créeraient tout de même un précédent alarmant : ils permettraient aux agents des forces de l'ordre et du renseignement de demander des renseignements sans mandat, sur la seule base d'un soupçon – plutôt que d'une croyance – que ces renseignements seraient utiles à une enquête criminelle. Ce précédent est inquiétant et risque d'ouvrir la voie à un élargissement des demandes sans mandat à mesure qu'elles se banaliseront.

Recommandation 1 : Que le comité examine en profondeur l'incidence des ordres de confirmer la fourniture de services sans mandat, qui créeraient un précédent.
Recommandation 2 : Que les articles 5 et 31 du projet de loi C-22 soient modifiés pour obliger les forces de l'ordre et le Service canadien du renseignement de sécurité (SCRS), le gouvernement fédéral, ou les deux, à publier chaque année un rapport sur le recours aux ordres de confirmer la fourniture de services.

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

L'article 6 du projet de loi C-22 créera un nouveau pouvoir d'« ordonnance de communication » permettant à la police d'obtenir des renseignements personnels (appelés « renseignements relatifs à l'abonné ») sur les clients de toute entité qui fournit un service au public, selon le seuil très bas des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise et que ces renseignements seront utiles à l'enquête sur cette infraction. Le seuil approprié serait plutôt la norme plus exigeante des « motifs raisonnables de croire », qui tient mieux compte de la nature délicate des renseignements en question et qui correspond à la norme actuellement appliquée à d'autres ordonnances semblables.

Ces préoccupations découlent de quatre aspects du projet de loi :

Premièrement, les renseignements visés par la définition de « renseignements relatifs à l'abonné » vont au-delà des renseignements de base sur les clients ou les abonnés : ils englobent des détails potentiellement très révélateurs, non seulement sur le client, mais aussi sur les services qu'il a utilisés, la période d'utilisation et les appareils employés. La définition vise :

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 pendant 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.

Non seulement ces renseignements en disent long sur la vie privée d'une personne, mais la liste n'exclut pas non plus d'autres données. Par exemple, les dates de naissance et les caractéristiques physiques pourraient aussi servir à identifier une personne; les identifiants détenus par un fournisseur de services pourraient permettre de révéler des renseignements

figurant dans une autre base de données; les types de services fournis et les dates de service pourraient révéler des projets de voyage, des antécédents médicaux ou des avoirs financiers.

Deuxièmement, cette nouvelle ordonnance de communication s'appliquerait à tout fournisseur de services, une catégorie d'entités beaucoup plus large que celle des « fournisseurs de services de télécommunication » visés par les ordres de confirmer la fourniture de services. Les « fournisseurs de services » pourraient ainsi englober aussi bien un professionnel ou une professionnelle de la santé qu'une agence de location de voitures, un fournisseur de services de courriel ou d'accès Internet ou une institution financière.

Troisièmement, cette nouvelle ordonnance de communication a une portée beaucoup plus large que les ordonnances de communication existantes assorties du seuil des « motifs raisonnables de soupçonner ». Par exemple, le paragraphe 487.018(1) du *Code criminel* établit un pouvoir d'ordonnance de communication visant des données financières. Une telle demande vise uniquement les institutions financières et établit une liste fermée des données pouvant être demandées (contrairement à la liste ouverte que contient la définition proposée de « renseignements relatifs à l'abonné »). Même si les données visées ressemblent aux « renseignements relatifs à l'abonné », cette ordonnance de communication ne peut servir à demander « tout » renseignement identificatoire, ni l'ensemble des services fournis, ni les appareils utilisés par une personne.

Enfin, l'article 7 du projet de loi C-22 permettrait aux forces de l'ordre de demander une autorisation judiciaire pour présenter une « demande » à des fournisseurs de services de télécommunication étrangers en vue d'obtenir des données de transmission ou des renseignements relatifs à l'abonné, là encore sur la base de « motifs raisonnables de soupçonner ». Ce nouveau pouvoir aura pour effet d'accroître considérablement la masse de renseignements personnels révélateurs auxquels les forces de l'ordre canadiennes peuvent accéder sur la base d'un seuil peu élevé; de plus, les règles de collecte et de conservation des données de certains pays étrangers pourraient être moins rigoureuses, ce qui menacerait encore davantage la protection de la vie privée.

> **Recommandation 3 :** Que les articles 6 et 7 du projet de loi C-22 soient modifiés par le remplacement de « motifs raisonnables de soupçonner » par « motifs raisonnables de croire ».

D'autres préoccupations subsistent à l'égard de la partie 1. Nous appuyons notamment les préoccupations que la Ligue des droits et libertés a soulevées dans son mémoire au sujet de la communication volontaire de renseignements et de l'utilisation de renseignements accessibles au public[4], ainsi que celles que l'Association canadienne des libertés civiles et le Citizen Lab ont soulevées dans leur mémoire au sujet des modifications du régime d'entraide juridique[5].

[4] Ligue des droits et libertés, *La mise en place d'une architecture de surveillance au Canada*, 29 octobre 2026.
[5] Cynthia Khoo, Tamir Israel et Kate Robertson, *(Un)forced Errors: Analysis of Proposed Surveillance Law Expansion under Bill C-22, An Act respecting lawful access*, Citizen Lab et Association canadienne des libertés civiles, 2 juin 2026.

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

La principale source de préoccupation dans le projet de loi C-22 est la création proposée, à la partie 2, de la Loi sur le soutien en matière d'accès autorisé à de l'information (LSAAI).

Au moyen de règlements publics comme d'arrêtés secrets, la LSAAI permettrait au gouvernement d'obliger la catégorie, définie en termes larges, des « fournisseurs de services électroniques » (FSE) à apporter à leurs systèmes des modifications vastes et radicales afin de faciliter l'accès des organismes d'application de la loi et de renseignement, ainsi qu'à conserver des données personnelles sensibles sur les personnes utilisatrices pendant au plus six mois, sans garanties suffisantes contre les vulnérabilités de sécurité que de tels arrêtés créeront. Ces vulnérabilités poseront des risques considérables pour la sécurité de l'information en ligne, notamment en rendant le chiffrement pratiquement inutile. Le nouveau régime manquerait également de dispositions adéquates en matière de reddition de comptes et de transparence.

Les dispositions de la LSAAI représentent l'un des élargissements les plus importants de l'appareil de surveillance étatique des 20 dernières années. Si elle est adoptée, la LSAAI menacera non seulement le droit à la vie privée, mais aussi des libertés connexes comme la liberté d'expression, la liberté d'association et les droits à l'égalité. Elle contribue 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 racisées 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 LSAAI sont en grande partie identiques à celles qui figuraient à l'origine dans le projet de loi C-2. Si le projet de loi C-22 introduit certaines nouvelles garanties, celles-ci sont contrebalancées, entre autres, par l'élargissement des pouvoirs de prendre des arrêtés à la conservation des métadonnées. De plus, les amendements adoptés à la Chambre des communes concernant le chiffrement, les vulnérabilités systémiques et les métadonnées ne parviennent toujours pas à parer adéquatement aux risques pour notre vie privée et notre sécurité. L'étude à la Chambre des communes a en outre souffert de sa précipitation : les comparutions de témoins ont été limitées, les débats ont été bâclés et les mémoires n'ont pas pu être distribués aux membres du comité en temps utile.

Compte tenu de tout ce qui précède et des préoccupations exposées ci-dessous, nous estimons que la partie 2 du projet de loi C-22 ne devrait pas recevoir la sanction royale et qu'elle devrait plutôt être retirée afin de faire l'objet d'une étude et de consultations plus approfondies.

Recommandation 4 : Veiller à ce que le projet de loi C-22 fasse l'objet d'une étude complète, au cours de laquelle seront entendus des spécialistes des libertés civiles, des droits de la personne, de la protection de la vie privée et de la cybersécurité.
Recommandation 5 : Retirer la partie 2, puisqu'il est impossible de la modifier de manière à respecter les droits garantis par la *Charte*.

Principaux problèmes de la partie 2 du projet de loi C-22

Problème 1 : La définition de « fournisseurs de services électroniques » a une portée inacceptable

Les pouvoirs de prendre des arrêtés et des règlements prévus par la LSAAI s'appliqueront à tous les FSE, que le projet de loi définit comme une « [p]ersonne qui, seule ou au titre de son appartenance à un groupe, fournit des services électroniques […] 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 ».

Le « service électronique » est quant à lui 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 ».

La LSAAI vise donc non seulement les grandes plateformes en ligne et les entreprises de télécommunication comme Meta, X, Amazon, Bell et Rogers, mais aussi les librairies de quartier, les fournisseurs de services de santé mentale, les institutions financières, les sites de réservation de voyages, les sites de rencontre et plus encore, c'est-à-dire pratiquement tout ce qui permet aux personnes utilisatrices de créer un compte, de communiquer ou de prendre rendez-vous en ligne. Certaines personnes se sont même demandé si les sites Web qui permettent simplement de publier des commentaires seraient aussi visés. Même les exploitants de réseaux Wi-Fi, comme les écoles, les bibliothèques et les cafés, pourraient être visés. Cette catégorie a une portée inacceptable, et le gouvernement n'a pas expliqué pourquoi il est nécessaire de viser un éventail aussi large d'entreprises.

Les FSE engloberont aussi une sous-catégorie appelée « fournisseurs principaux »; toutefois, ces derniers ne seront définis par règlement qu'après l'édiction de la LSAAI, de sorte qu'il est impossible de savoir avec certitude quels FSE en feront partie.

Les fournisseurs principaux seront assujettis à des règlements publics pris par le gouverneur en conseil. Si la publicité de ces règlements est un point positif, elle est toutefois compromise par le pouvoir du ministre de la Sécurité publique de prendre des arrêtés secrets visant tous les FSE, y compris les fournisseurs principaux. En raison de ce secret, il sera impossible de connaître la

véritable portée des arrêtés signifiés aux FSE, principaux ou non. Il existe certes des garanties – comme l'obligation de faire approuver les arrêtés secrets par le commissaire au renseignement avant leur prise d'effet –, mais, comme nous l'expliquons ci-dessous, elles ne vont pas assez loin.

> **Problème 2 :** Les pouvoirs de prendre des arrêtés menacent la vie privée et la sécurité en ligne

Les règlements publics comme les arrêtés ministériels secrets prévus par la LSAAI peuvent servir aux mêmes fins.

Ces fins sont notamment les suivantes :

- l'élaboration, la mise en œuvre […] et le maintien de leurs 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;
- la conservation de catégories de métadonnées pendant au plus six mois.

Ces pouvoirs sont exceptionnellement vastes, même pour des règlements publics, et à plus forte raison pour des arrêtés secrets. Ils pourraient être exercés de façons difficiles à prévoir, avec des conséquences – voulues ou non – qu'il demeure impossible d'anticiper pleinement.

Quatre zones de risque sont particulièrement préoccupantes :

2.1 Le projet de loi C-22 affaiblira la sécurité en ligne et rendra le chiffrement inutile

Premièrement, l'ampleur des mesures que les FSE peuvent être tenus de prendre par arrêté affaiblira la protection des communications privées et de la transmission de données en ligne. Il pourrait notamment s'agir d'obliger les FSE à ajouter à leurs réseaux de nouveaux points d'accès permettant la surveillance gouvernementale ou la collecte de données, ce qui créerait aussi des brèches que d'autres acteurs – des États étrangers aux pirates informatiques – pourraient exploiter à leurs propres fins.

Le plus préoccupant, toutefois, c'est que la LSAAI minerait le chiffrement au point de le rendre inutile. Le projet de loi C-22 permettrait au gouvernement d'ordonner aux entreprises de créer des portes dérobées, de contourner ou d'affaiblir le chiffrement, ou encore de déchiffrer des données chiffrées pour que les organismes d'application de la loi et de renseignement puissent y accéder. Comme l'a souligné la Fondation Mozilla, « il n'existe aucun moyen sûr de créer un accès exceptionnel aux données chiffrées qui ne puisse être utilisé que par l'acteur visé. Un

mécanisme d'accès créé pour les forces de l'ordre peut aussi être découvert, exploité ou détourné par des acteurs potentiellement malveillants[6]. »

Pour répondre à ces préoccupations, le gouvernement a modifié le projet de loi C-22 au cours des débats à la Chambre des communes afin d'y ajouter une réserve limitant le déchiffrement (par. 2(4)), qui interdirait aux arrêtés d'obliger un fournisseur de services à créer une clé de déchiffrement lorsqu'il n'en existe pas. Cette modification ne corrige toutefois pas adéquatement cette faille du projet de loi, puisqu'elle laisse toujours la porte ouverte à l'affaiblissement du chiffrement ou à la création de portes dérobées dans les communications chiffrées, entre autres outils de contournement du chiffrement.

La protection de nos renseignements et de nos communications privés en ligne est essentielle à l'exercice de l'ensemble des droits et libertés civiles connexes dans un écosystème devenu indispensable à nos activités quotidiennes. Le projet de loi C-22 menace clairement ces protections.

2.2 La conservation obligatoire des métadonnées porte atteinte au droit à la vie privée

La LSAAI permettrait aussi au gouvernement d'ordonner aux FSE de conserver les métadonnées des personnes utilisatrices pendant au plus six mois. Il s'agit certes d'une réduction par rapport à l'obligation initiale de conserver les métadonnées pendant au plus un an, mais cette mesure demeure un risque inacceptable pour le droit à la vie privée : elle impose la conservation de données privées sans autorisation judiciaire, oblige les FSE à élargir la portée des données qu'ils recueillent sur les personnes utilisatrices et crée une mine de renseignements personnels que pourraient chercher à exploiter des entreprises, des gouvernements étrangers, des acteurs malveillants, voire les organismes canadiens d'application de la loi et de renseignement eux-mêmes.

Obliger des entreprises privées à conserver des renseignements sur les personnes utilisatrices en vue d'une éventuelle utilisation par le gouvernement revient à enrôler des sociétés privées dans la collecte de données gouvernementale. Les métadonnées ne révèlent peut-être pas le contenu des communications, mais elles en disent tout de même très long sur notre vie privée : à qui nous parlons, où nous voyageons, quand nous menons nos activités. Elles peuvent aussi mettre au jour des réseaux entiers de relations en établissant qui parle à qui, pendant combien de temps, qui se rend aux mêmes endroits aux mêmes moments, et ainsi de suite. Cela peut donner lieu à des hypothèses problématiques, souvent biaisées, qui peuvent mener (et ont déjà mené) au profilage et au harcèlement.

L'obligation de conserver de telles données personnelles met donc en jeu l'article 8 de la *Charte canadienne des droits et libertés*, qui protège contre les fouilles, les perquisitions ou les saisies

---

[6] S. Windwehr et T. Stampelos, *Canada's bill C-22 threatens encryption, users' privacy and the security of digital economies*, Mozilla.org, 8 octobre 2026 [TRADUCTION].

abusives. Comme l'a souligné le professeur Michael Geist, il en résulterait « une carte de surveillance de presque toute la population canadienne[7] ». En aucun cas on ne devrait ordonner la conservation d'une telle quantité de renseignements personnels sans autorisation judiciaire. Même dans ce cas, l'autorisation de conserver des métadonnées pendant six mois devrait être considérée comme une mesure exceptionnelle assortie d'un lourd fardeau de la preuve.

Au-delà de ses incidences au regard de la *Charte*, la conservation obligatoire des métadonnées a aussi d'importantes conséquences pour la sécurité des données. Un tel réservoir de données serait une mine d'or pour les pirates informatiques, les entités étrangères et d'autres acteurs malveillants. Il se prêterait aussi aux abus de la part de personnes travaillant pour les entreprises qui recueillent les données ou de membres des forces de l'ordre y ayant accès, comme en témoignent de nombreux cas documentés d'agents qui ont utilisé à mauvais escient des bases de données existantes pour suivre d'ex-partenaires intimes ou des femmes qu'ils trouvaient attirantes.

2.3 Les arrêtés ministériels secrets minent la reddition de comptes et mettent en péril les droits et la sécurité

Comme nous l'avons mentionné, la LSAAI confère au ministre de la Sécurité publique le pouvoir de prendre des arrêtés secrets visant tous les FSE, y compris les fournisseurs principaux.

À l'origine, la LSAAI excluait toute communication de ces arrêtés, y compris leur contenu et le fait même qu'un arrêté avait été pris; or, les amendements adoptés à la Chambre des communes permettraient désormais au ministre d'y inclure « toute disposition relative à la communication d'information contenue dans [l'arrêté] et à la communication du fait que le fournisseur de services électroniques y est assujetti » (par. 7(1.1)).

Cette modification laisse toutefois encore au ministre un pouvoir discrétionnaire trop large pour décider quand et comment la communication est permise. Aucun facteur n'encadre ce dont le ministre doit tenir compte, et aucun motif ne précise pourquoi des renseignements devraient demeurer secrets. Même avec de telles lignes directrices, le pouvoir discrétionnaire du ministre resterait trop étendu. C'est d'autant plus vrai que ce seraient vraisemblablement les arrêtés les plus controversés, ou ceux qui présentent les plus grands risques pour la vie privée ou la cybersécurité, qui ne seraient pas communiqués.

Problème 3 : L'utilisation possible de ces pouvoirs et les risques connexes

Les pouvoirs que la LSAAI confère aux organismes d'application de la loi et de renseignement sont exceptionnellement vastes, surtout dans le cas des arrêtés ministériels pris en secret. Ils pourraient être exercés de façons difficiles à prévoir, avec des conséquences – voulues ou non –

[7] *Op. cit.*, note 3 [TRADUCTION].

qu'il demeure impossible d'anticiper pleinement. Nous pouvons toutefois déjà envisager certains risques :

- Expansion rapide des pouvoirs de surveillance de l'État. Nous avons déjà vu de nouveaux pouvoirs de surveillance, surtout ceux exercés en secret, s'étendre au fil du temps et entraîner une surveillance illégale et des violations de droits.
- Une fois en place, les portes dérobées et les systèmes de surveillance ne servent pas seulement aux organismes canadiens d'application de la loi et de renseignement ou aux alliés du Canada :
    - Les organismes étrangers d'application de la loi ou de renseignement, quels qu'ils soient, peuvent aussi y accéder et les exploiter.
    - Ils peuvent être exposés à des attaques, à du piratage, à des fuites ou à des utilisations abusives.
    - L'attaque « Salt Typhoon » de 2023-2024 en est un exemple marquant : elle a exploité des portes dérobées et des points d'accès destinés à faciliter les capacités d'interception des services de sécurité nationale des États-Unis.

Enfin, les exemples fournis par le gouvernement ne permettent pas de saisir toute l'étendue des utilisations que les organismes d'application de la loi et de renseignement, canadiens comme étrangers, pourraient faire de ces renseignements. Parmi les scénarios présentés par le gouvernement figurent le repérage de téléphones utilisés par des terroristes présumés, la localisation et le sauvetage en toute sécurité d'enfants enlevés et l'identification de personnes anonymes se livrant à l'exploitation sexuelle de mineurs. Or, les utilisations possibles vont bien au-delà :

- Les données de localisation et de communication offriraient encore plus de possibilités de suivre et de surveiller des défenseurs et défenseuses autochtones du territoire ou d'autres militants et militantes, comme l'a récemment révélé la CBC. Les gouvernements pourraient s'en servir pour cibler tout segment de la population qu'ils jugent menaçant pour leurs politiques (que cette menace comporte ou non un réel risque de violence).
- Ces données pourraient aussi servir à suivre, à la manière des États-Unis, les personnes immigrantes et réfugiées ainsi que les citoyens et citoyennes naturalisés et racisés, afin de faciliter leur détention et leur expulsion.
- La collecte et l'organisation de métadonnées sur des Canadiens et Canadiennes et sur des personnes étrangères profiteraient grandement aux pouvoirs de collecte d'ensembles de données du SCRS. Depuis leur adoption en 2019, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a déjà critiqué ces pouvoirs, qui sont exercés de façons inédites et sans reddition de comptes.
- L'accès des forces de l'ordre étrangères, notamment américaines, à ces données à des fins d'enquêtes et de poursuites qui menacent des communautés entières, par exemple les personnes qui cherchent à obtenir un avortement ou d'autres soins de santé reproductive, ou encore des soins d'affirmation de genre (y

compris les citoyens et citoyennes des États-Unis qui obtiennent légalement de tels soins au Canada).

Problème 4 : Des garanties inadéquates et un secret injustifié

La LSAAI comporte certes des garanties intégrées, mais celles-ci sont nettement insuffisantes.

4.1 Vulnérabilités systémiques

Parmi les principales protections invoquées par le gouvernement figure la disposition de la LSAAI selon laquelle un fournisseur principal ne serait pas tenu de se conformer à un règlement, et un FSE ne serait pas tenu de se conformer à un arrêté, si cela avait pour effet de l'obliger à introduire une vulnérabilité systémique dans son service ou de l'empêcher de corriger une telle vulnérabilité.

Or, la définition de « vulnérabilité systémique » au paragraphe 2(1) de la LSAAI comporte de graves lacunes et soulève plusieurs préoccupations importantes. Le plus alarmant, c'est qu'elle n'empêche pas l'introduction de vulnérabilités : elle exclut seulement celles qui présenteraient un « risque crédible » d'accès par des personnes non autorisées, et uniquement lorsque l'information ne se rapporte pas à des personnes visées par un mandat ou un autre pouvoir d'accéder à de l'information. Ce raisonnement repose toutefois sur la prémisse que l'accès à de telles vulnérabilités peut être limité aux personnes autorisées. Le gouvernement affirme que le seuil sera un « risque crédible » qu'une personne non autorisée puisse accéder à l'information, mais il s'agit d'une norme très subjective, qui laisse planer une réelle possibilité que la tentation de créer des vulnérabilités utiles à la sécurité nationale ou à l'application de la loi entraîne l'érosion progressive de ce seuil. On ignore aussi sur quelles « normes techniques internationales » reposera la décision, ce qui n'offre guère l'assurance d'une norme rigoureuse et uniforme. Enfin, comme l'ont montré les cyberattaques Salt Typhoon et de récents exemples d'outils d'intelligence artificielle qui ont détecté et exploité des failles de cybersécurité, il est extrêmement difficile, voire impossible, de mesurer le risque futur d'accès non autorisé que créent les vulnérabilités.

4.2 Les obligations de rapport ne remplacent pas une surveillance efficace

Comme nous l'avons expliqué, la portée du secret et des ordonnances de non-communication est inacceptable. Les arrêtés ministériels secrets peuvent viser toute la gamme des modifications des systèmes des FSE, des plus anodines aux plus importantes; comme on peut s'y attendre, ce sont les arrêtés les plus délicats et les plus controversés qui seront pris en secret. Le ministre de la Sécurité publique aura le pouvoir de déterminer si une quelconque communication de l'arrêté est possible, qu'il s'agisse de son contenu ou même de son existence. Le commissaire au renseignement examinera le caractère raisonnable des arrêtés, mais on ne sait pas si cet examen portera aussi sur les motifs invoqués par le ministre pour

justifier la non-communication. Compte tenu de la portée des pouvoirs de prendre des arrêtés en question, un tel degré de secret et de pouvoir discrétionnaire est inacceptable.

La portée et les répercussions des arrêtés secrets justifient un contrôle judiciaire, et non un simple examen par le commissaire au renseignement. Même si le commissaire au renseignement est un juge à la retraite qui exerce ses fonctions de façon indépendante, la solidité du poste dépend entièrement de la personne nommée. Comme la nomination relève du gouvernement, le poste demeure exposé à une éventuelle politisation ou à des compressions budgétaires. De plus, les délibérations se déroulent en secret, et les rapports publics sont strictement limités. Compte tenu des pouvoirs considérables que la LSAAI confère au gouvernement, le Bureau du commissaire au renseignement n'est pas l'instance appropriée pour approuver les arrêtés ministériels; seul un contrôle judiciaire offrirait la certitude nécessaire, si tant est que l'on accepte des arrêtés secrets.

Les obligations de rapport public, l'échange d'information avec l'OSSNR et l'examen obligatoire trois ans après l'édiction du régime de la LSAAI ne dissipent pas non plus ces préoccupations. Si la production de rapports et l'examen sont nécessaires à tout régime de ce genre, ils ne permettent de répondre aux préoccupations qu'une fois l'arrêté pris et n'offrent aucune garantie avant son exécution.

Conclusion

En réaction au projet de loi C-2, des centaines d'organisations de la société civile ont dénoncé le fait que les nouveaux pouvoirs de surveillance prévus portaient gravement atteinte aux droits fondamentaux au Canada. Si le projet de loi C-22 tente modestement de répondre à ces préoccupations, il continue de présenter un risque non seulement pour le droit à la vie privée, mais aussi pour un large éventail de droits connexes qui dépendent de la possibilité de communiquer en privé, à l'abri de toute surveillance et de toute ingérence gouvernementales injustifiées. Le projet de loi C-22 crée aussi, sans justification, des risques de cybersécurité qui menaceront davantage les renseignements privés non seulement des personnes qui se trouvent au Canada, mais aussi de toutes les personnes dont les données sont détenues par des FSE assujettis au nouveau régime de règlements et d'arrêtés secrets créé par la LSAAI. Au cours des derniers mois, les spécialistes de la protection de la vie privée et les défenseurs et défenseuses des libertés civiles au Canada ont été rejoints par des spécialistes de l'étranger, des entreprises technologiques et des législatrices et législateurs, qui réclament eux aussi que le gouvernement change de cap concernant le projet de loi C-22.

Compte tenu de ces préoccupations, notre coalition demande aux sénateurs et sénatrices de rejeter le projet de loi C-22 et de voter contre. À défaut, il faut apporter des amendements importants à la partie 1 et retirer la partie 2.