PROJET DE LOI C-22

LOI CONCERNANT L'ACCÈS LÉGAL

LA MISE EN PLACE D'UNE ARCHITECTURE DE SURVEILLANCE AU CANADA

MÉMOIRE PRÉSENTÉ PAR

AU COMITÉ PERMANENT DE LA SÉCURITÉ PUBLIQUE ET NATIONALE

CHAMBRE DES COMMUNES DU CANADA

20 MAI 2026

PRÉSENTATION DE LA LIGUE DES DROITS ET LIBERTÉS

La Ligue des droits et libertés (LDL) est une organisation indépendante, non partisane et sans but lucratif, qui vise à défendre et à promouvoir les droits humains en mettant de l'avant leur universalité, leur indivisibilité et leur interdépendance. Depuis sa création en 1963, la LDL a influencé plusieurs politiques gouvernementales et projets de loi en plus de contribuer à la création d'instruments et d'institutions voués à la défense et la promotion des droits humains, tels que la *Charte des droits et libertés de la personne* du Québec et la Commission des droits de la personne et des droits de la jeunesse (CDPDJ).

Elle intervient régulièrement dans l'espace public pour porter des revendications et dénoncer des violations de droits humains auprès des instances gouvernementales sur la scène locale, nationale ou internationale. La LDL est également membre de la Fédération internationale pour les droits humains (FIDH). La LDL poursuit, comme elle l'a fait tout au long de son histoire, différentes luttes contre la discrimination et contre toute forme d'abus de pouvoir, pour la défense des droits civils, politiques, économiques, sociaux et culturels qui sont universels, interdépendants et indissociables.

Par la présente, la LDL transmet son mémoire au Comité permanent de la Sécurité publique et nationale de la Chambre des communes sur le projet de loi C-22, *Loi concernant l'accès légal*, déposé le 12 mars 2026.

INTRODUCTION

Le projet de loi C-22, *Loi concernant l'accès légal*, déposé par le gouvernement le 12 mars 2026 met en place une architecture de surveillance sans précédent qui pourrait affecter chaque outil numérique que les Canadien·nes utilisent au quotidien. Ce projet de loi représente l'une des plus grandes menaces au droit à la vie privée au Canada des deux dernières décennies.

C-22 contient de vastes nouveaux pouvoirs qui pourraient obliger tout fournisseur de services numériques à conserver pour une période d'un an les métadonnées de chaque client au Canada, portant ainsi atteinte à la vie privée de millions de personnes. La portée absolument excessive de C-22 constitue une menace grave pour les libertés civiles.

Que des pays partenaires du Canada aient adopté de telles dispositions ne justifie en rien la mise sur pied d'un État de surveillance et l'abandon de nos principes démocratiques et de nos droits constitutionnels. Bien au contraire, les dérives et abus qui accompagnent de telles dispositions appellent la Ligue des droits et libertés à demander le rejet sans équivoque de ce projet de loi liberticide.

PARTIE 1 DU PROJET DE LOI C-22

Le projet de loi C-22 introduit d'importantes modifications au *Code criminel* et à la *Loi sur le Service canadien du renseignement de sécurité* (SCRS). Les modifications proposées élargissent grandement les pouvoirs des organismes d'application de la loi (policiers et fonctionnaires publics) et du SCRS dans l'obtention de renseignements relatifs aux abonnés (RRA) et de données de transmission (DT).

1. ORDRE DE CONFIRMER LA FOURNITURE DE SERVICES

Le projet de loi C-2 (première mouture de C-22) aurait permis l'accès aux RRA, sans mandat judiciaire, dans le cadre d'un ordre de fournir des renseignements. Le gouvernement a reculé sur ce point. Avec C-22[1], il s'agit plutôt d'un ordre de confirmer la fourniture de services (OCFS) visant uniquement le fournisseur de services de télécommunications (FST) et se limitant à la question de savoir s'il fournit ou non des services à un·e abonné·e.

Bien que la catégorie des FST soit plus restreinte que « toute personne fournissant des services au public », comme c'était le cas dans C-2, à l'ère numérique, elle demeure vaste : opérateurs mobiles, plateformes de messagerie, réseaux sociaux, services d'infonuagique, etc.

Ainsi, la portée de ce nouveau pouvoir demeure préoccupante d'autant plus que ce dernier échappe à la surveillance judiciaire. En effet, l'OCFS peut être émis sur la base de simples soupçons (motifs raisonnables de *soupçonner*) qu'une infraction à une loi fédérale (n'importe quelle infraction) a été ou sera commise et que les renseignements seront utiles à l'enquête – le tout évalué uniquement selon l'agent policier et non confirmé par un·e juge. Notons que la norme des motifs raisonnables de *soupçonner* est plus basse que la norme des motifs raisonnables de *croire*.

De plus, l'ordre peut être accompagné d'une interdiction de divulgation pouvant aller jusqu'à un an. Le fait que l'information reçue sur la base de cet OCFS pourra servir éventuellement à obtenir une ordonnance de communication (section suivante) crée un effet d'escalade : un pouvoir sans surveillance judiciaire devient le point d'entrée vers l'exercice d'un autre pouvoir permettant l'obtention de renseignements beaucoup plus substantiels.

2. ORDONNANCE DE COMMUNICATION ET RENSEIGNEMENTS RELATIFS À L'ABONNÉ·E

Les RRA pourront être obtenus par Ordonnance de communication[2] (OCRRA) émise par un·e juge. Cet ordre est adressé à toute « personne fournissant des services au public (PFSP) ». Le champ d'application est donc extrêmement vaste. Les RRA sont, eux aussi, définis très largement : nom, adresse, numéro de téléphone, adresse courriel, pseudonyme, identifiant, numéro de compte, les services fournis (types, période, équipements utilisés)[3]. Ces renseignements très sensibles pourront être obtenus sur la base de motifs raisonnables de *soupçonner* qu'une infraction à n'importe quelle loi fédérale a été ou sera commise. Et sur simple démonstration qu'ils seraient « *utiles* à l'enquête ».

---

[1] Projet de loi C-22, articles 5 et 31.

[2] Projet de loi C-22, article 6.

[3] Projet de loi C-22, article 4.

Il s'agit d'un abaissement inacceptable de la norme applicable à ce type de fouille depuis l'arrêt *Spencer* de la Cour suprême[4]. Actuellement, c'est par une ordonnance générale de communication (OGC)[5] que les autorités peuvent obtenir les RRA[6]. Et c'est la norme plus contraignante des motifs raisonnables de *croire* qui est alors exigée. Qui plus est, dans ce cadre, la personne requérante doit démontrer que les RRA « fourniront une preuve concernant la perpétration de l'infraction » et non qu'ils seront simplement « utiles à l'enquête » comme le propose C-22. Il s'agit d'un recul majeur en regard de la protection de la vie privée des citoyen·nes.

Ces dernières années, la Cour suprême a établi, dans les arrêts *Spencer* et *Bykovets*[7], l'importance à accorder aux RRA en lien avec une activité en ligne. Dans *Spencer*, la Cour reconnaît « que l'anonymat constitue une protection importante des droits en matière de vie privée à l'égard des activités en ligne[8] ». Des attentes raisonnables au respect de la vie privée existent en regard de ces informations et l'abandon de la norme des motifs raisonnables de *croire* compromet gravement ce droit fondamental.

Nos commentaires précédents s'appliquent aux pouvoirs similaires accordés au SCRS par les articles 30 à 36 de C-22.

3. COLLABORATION

L'article 11 de C-22 amenderait le *Code criminel*[9] pour « préciser » qu'aucune ordonnance n'est nécessaire pour qu'un agent de la paix puisse *demander* à une *personne* de lui « fournir *volontairement* des renseignements qu'aucune règle de droit n'interdit à celle-ci […] de communiquer » (nous soulignons). La personne qui collabore bénéficie alors « de l'immunité en matière civile ou pénale ». Aucune limite n'est édictée quant au type de renseignements visés. Cela inclut-il les renseignements personnels, notamment des RRA? On peut le craindre.

Dans l'arrêt *Spencer*, la Cour suprême a pourtant déterminé que la *demande* de RRA formulée par un policier constitue une fouille[10]. L'arrêt *Bykovets* réaffirme ce principe.

> Dans *Spencer*, notre Cour a jugé qu'une attente raisonnable au respect de la vie privée s'applique aux renseignements relatifs à l'abonné — les nom, adresse et coordonnées — associés à l'adresse de protocole Internet (IP) d'une personne. Une demande de l'État en vue

---

[4] *R c. Spencer*, 2014 CSC 43.

[5] Code criminel L.R.C. 1985, ch. C-46, art. 487.014.

[6] « Depuis l'arrêt rendu par la Cour suprême du Canada dans l'affaire R c Spencer [2014], l'ordonnance générale de communication est le seul outil dont dispose la police pour obtenir les renseignements sur les personnes abonnées. » Gouvernement du Canada. Modifications proposées aux lois sur l'accès aux renseignements en temps opportun (Projet de loi C-22, Partie 1). https://www.justice.gc.ca/fra/sjc-csj/pl/c22/index.html

[7] *R. c. Bykovets*, 2024 CSC 6.

[8] *R. c. Spencer*, 2014 CSC 43, para 78.

[9] Remplacement de l'article 487.0195.

[10] *R. c. Spencer*, op. cit., par 66. « À mon avis, compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. […] La demande faite par la police visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille.

> d'obtenir ces renseignements constitue une « fouille » ou « perquisition » au sens de l'art. 8 de la *Charte canadienne des droits et libertés*.[11]

Les modifications prévues par l'article 11 permettraient éventuellement de contourner ces deux arrêts en soustrayant de la surveillance judiciaire les échanges volontaires de RRA, entre la police et les personnes.

Certes il y a une réserve : la fourniture de renseignement est conditionnelle à ce qu'aucune règle de droit ne l'interdise. Mais pourquoi, dans ce cas, accorder une immunité civile ou pénale à la personne? Cela apparaît incohérent. On peut redouter que la personne, vu cette immunité civile ou pénale, mette peu ou pas d'efforts pour vérifier si la remise d'information est légalement permise.

Ces modifications mettent en péril le droit à la vie privée en ligne. Elles assurent une protection à des échanges laissés au bon vouloir des personnes ou sociétés privées, et mènent à une forme d'arbitraire. Dans *Bykovets*, la Cour souligne l'importance d'une supervision judiciaire :

> La surveillance judiciaire enlèverait également aux sociétés privées le pouvoir de décider s'il convient de révéler des renseignements — et en quelle quantité — et renverrait la question au champ d'application de la Charte.[12]

4. RENSEIGNEMENTS ACCESSIBLES AU PUBLIC

L'article 11 de C-22 apporte un autre changement au *Code criminel*. Il énonce qu'aucune ordonnance n'est nécessaire pour « recevoir ou obtenir des renseignements accessibles au public et y donner suite ». Aucune définition de « renseignements accessibles au public » n'est prévue ni aucune limite n'est fixée dans leur utilisation.

Vise-t-on ici, notamment, des renseignements obtenus sur le web? Dans l'affaire Clearview AI[13], le Commissariat à la protection de la vie privée du Canada et ses homologues provinciaux ont statué qu'un renseignement personnel provenant de sources telles que les médias sociaux ou les profils professionnels ne pouvait être utilisé sans le consentement de la personne concernée, et ce, en vertu des lois de protection des renseignements personnels. Comme le soulignait la Commission d'accès à l'information du Québec dans cette décision collégiale :

> [M]ême si un renseignement personnel est diffusé sur un site public, cela ne veut pas dire que ce renseignement peut être utilisé à d'autres fins sans le consentement de la personne concernée. La publication d'images sur un site Web ne signifie pas forcément que son auteur consent à ce qu'elles soient utilisées par un tiers[14].

---

[11] *R. c. Bykovets*, 2024 CSC 6, para 2.

[12] *R. c. Bykovets*, 2024 CSC 6, para 12.

[13] Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta. Conclusions en vertu de la LPRPDE n° 2021-001. 2 février 2021. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/

[14] Ibid., para 46.

Les commissaires ont donc conclu que le logiciel de reconnaissance faciale élaboré par Clearview AI à partir de photos prises sur le net – sans consentement – était illégal; tout comme il était illégal pour la Gendarmerie royale du Canada (GRC) d'utiliser un tel logiciel[15].

Donner aux forces policières la possibilité d'utiliser sans limites l'information disponible sur le Web, seulement parce qu'elle est « accessible », comporte de graves risques :

> Les Canadiens doivent être libres de participer volontairement et activement aux activités courantes d'une société moderne, qui sont de plus en plus numériques. Ils doivent être en mesure de circuler dans les espaces publics, semi-publics et privés sans risquer que leurs activités soient systématiquement recensées, suivies et surveillées.[16]

Comme le rappelle la Cour suprême dans *Bykovets* « les Canadiens n'ont pas à vivre en reclus du monde numérique afin de pouvoir conserver un semblant de vie privée[17] ».

La loi devrait prévoir spécifiquement les renseignements pouvant être utilisés par les forces policières. La modification proposée par C-22 quant aux renseignements accessibles au public est beaucoup trop large. Elle pourrait saper les principes établis dans Clearview AI. À tout le moins devrait-on préciser que le pouvoir d'obtenir et de donner suite à un renseignement accessible au public doit s'exercer sous réserve des lois de protection des renseignements personnels.

5. POUVOIRS ÉLARGIS EN CAS D'« URGENCE »

L'article 14 de C-22 propose de modifier l'article 487.11 du *Code criminel* et élargir de manière considérable les pouvoirs qui seront possibles lorsque « l'urgence de la situation rend difficilement réalisable l'obtention du mandat ». Actuellement, en situation d'urgence, un agent peut, sans mandat, avoir le pouvoir de perquisition de type général, prévue à l'art. 487, ainsi que le pouvoir de mettre un dispositif de localisation sur une chose, prévu à l'art. 492.1. Si la modification est adoptée, en plus de ces pouvoirs, les policiers pourraient *sans mandat* :

- Installer un dispositif de localisation sur une personne, pouvoir prévu à l'art. 492.1 (2), nécessitant habituellement un mandat sur la base des motifs raisonnables de *croire*;
- Installer un enregistreur de données de transmission, pouvoir prévu à l'art. 492.2 (1) ;
- Obtenir la communication des données de transmission, pouvoir prévu à l'art. 487.016;
- Obtenir la communication des données de localisation, pouvoir prévu à l'art 487.017;
- Ainsi que le nouveau pouvoir à l'article 487.0142 sur la communication des RRA.

---

[15] Commissariat à la protection de la vie privée du Canada. « L'utilisation par la GRC de la technologie de reconnaissance faciale de Clearview AI contrevenait à la *Loi sur la protection des renseignements personnels*, selon une enquête ». Communiqué. 10 juin 2021. https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2021/nr-c_210610/

[16] Commissariat à la protection de la vie privée du Canada. « Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée ». https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/

[17] *R. c. Bykovets*, op. cit., par. 48.

Notons en particulier que le pouvoir d'installer sans mandat un dispositif de localisation sur une personne, et non sur une chose, permet de suivre les déplacements d'un individu en temps réel, le tout sans aucune autorisation judiciaire (aujourd'hui requise sur la base de motifs raisonnables de *croire*), sur la seule appréciation de l'agent que l'urgence de la situation le justifie, et sans que la personne visée n'en soit jamais informée.

6. DEMANDE DE COMMUNICATION À UNE ENTITÉ ÉTRANGÈRE

L'article 7 de C-22 modifie le Code *criminel* par l'ajout d'un nouvel article.[18] Il permettrait aux organismes d'application de la loi de demander « à une entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de communication » de communiquer des RRA et des données de transmission en sa possession. La demande doit être autorisée par un·e juge selon la norme des motifs raisonnables de *soupçonner* une infraction à une loi fédérale et que les renseignements seraient utiles à l'enquête.

Il va de soi que nos critiques formulées au point 1 sur l'utilisation d'une norme moins rigoureuse dans l'obtention de RRA et de DT – plutôt que la norme des motifs raisonnables de *croire* – s'appliquent ici.

7. LOI SUR L'ENTRAIDE JURIDIQUE EN MATIÈRE CRIMINELLE (LEJMC)

L'article 29 de C-22 ajoute un nouvel article 22.07 à la LEJMC. Il permettrait aux autorités canadiennes d'assurer l'exécution de décisions étrangères en vue de l'obtention de RRA et DT conservés au Canada. La demande d'entraide est présentée au ministre de la Justice qui désigne une autorité compétente (Procureur général du Canada ou d'une province) pour présenter une requête à un·e juge. Le juge pourra rendre la décision étrangère exécutoire si elle remplit – *avec les adaptations nécessaires* – les conditions de 487.016 (2) dans le cas des DT; et de 487. 0142 (2) dans le cas des RRA, et donc, sur la base de motifs raisonnables de *soupçonner* une infraction et que les renseignements seront utiles.

Encore une fois, nos critiques formulées au point 1 sur l'utilisation d'une norme moins rigoureuse dans l'obtention de RRA et de DT – plutôt que la norme des motifs raisonnables de *croire* – s'appliquent ici, et a fortiori, puisqu'il s'agit de transmettre des renseignements personnels sensibles à une entité étrangère.

Par ailleurs, pour remplir les conditions de 487.016 (2) ou 487.0142 (2) il faut établir des motifs raisonnables de *soupçonner* une *infraction à une loi fédérale***.** Qu'en est-il dans le cas de l'exécution d'une décision étrangère? L'article précise « avec les adaptations nécessaires ». Mais qu'est-ce à dire? Entend-on permettre l'exécution de décisions étrangères pour des infractions inconnues au Canada? Ou pire encore pour des actes constituant au Canada l'exercice de droits démocratiques, mais considérés à l'étranger comme un crime? Le professeur Pierre Trudel résume fort bien le problème :

[18] Article 487.0181

> Est-il raisonnable de permettre à la police américaine d'obtenir des informations sur les personnes se trouvant au Canada ? Cela pourrait viser notamment des renseignements relatifs à des questions comme l'accès à l'avortement, les soins de réinsertion sociale ou les manifestations politiques.[19]

L'article 29 pave la voie à la multiplication d'échanges de renseignements personnels avec des États n'ayant pas le même corpus législatif et ne présentant pas nécessairement les mêmes garanties que le Canada au plan des droits humains et de la démocratie. De tels échanges pourraient mettre en danger la sécurité des personnes, qu'on pense par exemple à l'affaire Maher Arar[20]. La Ligue des droits et libertés s'oppose à l'élargissement des échanges transfrontaliers de données, en l'absence d'un cadre assurant la protection de la vie privée et le respect des droits.

8. DES MODIFICATIONS EN VUE D'AUTRES ATTEINTES À LA VIE PRIVÉE

C-22, à l'instar de son précédent C-2, semble de surcroît préparer la voie à un processus pour faciliter l'accès des entités étrangères aux données des Canadien·nes. Les dispositions modifiant la LEJMC viseraient notamment à répondre aux obligations découlant de la ratification du Deuxième protocole additionnel à la Convention de Budapest sur la cybercriminalité (2PA). Des fonctionnaires de Justice Canada ont d'ailleurs reconnu que l'intention de certaines dispositions de C-2, reprises dans C-22, était précisément de permettre au Canada de mettre en œuvre et de ratifier le 2PA. Ces dispositions pourraient également constituer une réforme préalable à un éventuel accord bilatéral Canada–États-Unis en vertu du Cloud Act américain. Or, ces deux instruments soulèvent des préoccupations importantes en matière de vie privée et de droits fondamentaux.

PARTIE 2 DU PROJET DE LOI C-22

La Partie 2 édicte la *Loi sur le soutien en matière d'accès autorisé à l'information*.

Sous couvert de « faciliter l'exercice efficace […] en matière d'accès à de l'information[21] » à des personnes chargées de l'application de la loi et de la sécurité nationale, C-22 instaure un système de surveillance de masse sans précédent, alors qu'aucune démonstration n'a été faite que les pouvoirs existants sont insuffisants.

1. FOURNISSEURS PRINCIPAUX

C-22 permet au gouverneur en conseil d'imposer par réglementation aux fournisseurs principaux de services électroniques d'élaborer, de mettre en œuvre et de maintenir des capacités opérationnelles et techniques pouvant permettre à la personne autorisée d'accéder à de l'information (art. 5(2)). Ces

---

[19] Pierre Trudel. « À la merci de la police de Trump ». *Le Devoir*. 19 août 2025. https://www.ledevoir.com/opinion/chroniques/910500/chronique-merci-police-trump

[20] Radio-Canada. Maher Arar blanchi, la GRC blâmée. 18 septembre 2006. https://ici.radio-canada.ca/nouvelle/322183/maher-blanchi

[21] Projet de loi C-22, Sommaire.

dispositions ont pour effet de mettre les fournisseurs de services électroniques au service des forces policières et de détourner les services qu'ils offrent à la population à des fins de surveillance.

Notons que la liste des « fournisseurs principaux » de services électroniques en annexe de la loi est vide et que le gouverneur en conseil peut par règlement « modifier l'annexe pour ajouter, modifier ou supprimer une catégorie de fournisseurs de services électroniques[22] ». Dans un manque total de transparence, la loi serait donc adoptée sans que le législateur ou la population aient la moindre idée de l'étendue des services qui seront éventuellement couverts. Ceci est d'autant plus inquiétant que la définition de fournisseur de services électroniques englobe toutes les « personnes qui […] fournissent des services électroniques, *notamment* en vue de permettre la communication[23] » (notre souligné). La loi permet donc d'assujettir des fournisseurs de services électroniques dont la fonction principale n'est pas de permettre la communication.

La définition de service électronique est par ailleurs très large : « Tout 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 combinaison de tels moyens.[24] »

Dans le monde numérique d'aujourd'hui, à peu près toutes les organisations avec lesquelles les Canadien·nes font affaire rentrent dans ces définitions. C-22 va permettre à l'État d'obliger arbitrairement une quantité innombrable d'entités auxquelles la population a recours à devenir des instruments à la disposition de l'État pour l'obtention d'information sur leurs client·es.

Les fournisseurs de services « principaux » pourront être obligés de conserver pour une période d'un an des catégories de métadonnées, *y compris* des données de transmission au sens de l'article 487.011 du *Code criminel*. En vertu de 487.011, les données de transmission sont des données qui, à la fois « concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication […] et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication ». Ces données ne sont pas banales. Elles révèlent énormément sur nos activités (liens sociaux, déplacements, etc.) et sont protégées par le droit à la vie privée.

De plus, la loi reste ouverte à ce que ces métadonnées ne se limitent pas aux données de transmission. Avec C-22 ces données seront compilées sur des personnes – potentiellement une partie importante de la population du Canada -- qui ne font l'objet d'aucune enquête. Elles seront accessibles aux forces de l'ordre et au SCRS sur la base de simples motifs raisonnables de *soupçonner*, alors que ces données devraient être accessibles aux forces de l'ordre dans le cadre d'enquêtes spécifiques avec un mandat judiciaire sur la base de motifs raisonnables de *croire*. C-22 est une attaque non seulement à la vie privée mais aussi à la présomption d'innocence.

[22] Projet de loi C-22, Partie 2, article 5 (1).
[23] Projet de loi C-22, Partie 2, article 2 (1).
[24] Ibid.

2. ARRÊTÉS MINISTÉRIELS

C-22 va encore plus loin. Le ministre peut prendre des arrêtés (art. 7(1)) à l'égard de fournisseurs de services, qu'ils soient fournisseurs principaux ou non, qui leur imposent les mêmes obligations que celles imposées aux services principaux par voie réglementaire. Cependant, la rétention d'information des arrêtés ministériels n'est pas assujettie aux mêmes restrictions que celle par voie réglementaire à 5(4). L'information visée par les arrêtés ministériels n'exclut pas explicitement le contenu de la communication, l'historique de navigations Web d'une personne ainsi que les activités d'une personne sur les médias sociaux. La somme de ces informations revient, à toute fin pratique, à une surveillance totale de la vie d'une personne. Les arrêtés pris en vertu du paragraphe 7(1) l'emportent sur tout règlement incompatible pris en vertu du paragraphe 5(2), et il est prévu qu'ils doivent demeurer secrets.

Un arrêté est valide au moment où le commissaire au renseignement l'approuve. En vertu de la Loi sur le SCRS, le ministre « peut déterminer une catégorie d'ensembles de données canadiens dont la collecte est autorisée s'il conclut que l'exploitation ou l'interrogation d'ensembles de données visés par cette catégorie permettra de générer des résultats pertinents ». Ces informations peuvent être recueillies sans autorisation judiciaire si elles sont approuvées par le commissaire au renseignement. Le projet de loi C-22 a pour but de rendre ces ensembles de données accessibles au SCRS en obligeant une liste élargie de fournisseurs – au-delà des fournisseurs principaux – à fournir des informations – au-delà de celles qui peuvent être obtenues par réglementation – au SCRS.

Les personnes assujetties à cette surveillance ne le sont pas dans le cadre d'une enquête criminelle, ignorent qu'elles sont l'objet d'une telle surveillance et n'ont pas de recours judiciaire. La seule protection contre les abus est l'obligation de faire approuver les arrêtés par le commissaire au renseignement, un processus qui se déroule dans le secret. Soulignons que le commissaire au renseignement doit prendre ses décisions sur la base d'informations fournies uniquement par les services de renseignement et le ministre.

3. OBLIGATION DE PRÊTER ASSISTANCE

Le gouverneur en conseil peut prendre des règlements obligeant les fournisseurs de services principaux de maintenir des « capacités opérationnelles et techniques, notamment en ce qui touche l'extraction et l'organisation de l'information à laquelle l'accès est autorisé[25] » et de veiller à « l'installation, l'utilisation, le fonctionnement, la gestion, la mise à l'essai 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[26] ».

Ces dispositions obligent les fournisseurs de service à maintenir des portes dérobées qui permettent aux personnes autorisées d'avoir accès aux informations détenues par les fournisseurs de services. La loi prévoit que le fournisseur n'est pas tenu de se conformer à la disposition d'un règlement si cela crée un risque sérieux qu'une personne non autorisée puisse avoir accès à l'information. Le projet de loi laisse complètement indéfini ce qui constitue un risque « sérieux ».

[25] Projet de loi C-22, Partie 2, article 5 (2) a).
[26] Projet de loi C-22, Partie 2, article 5 (2) b).

Mais là n'est pas la question. Toute vulnérabilité introduite dans des systèmes de données est inacceptable. L'expérience a démontré à quel point les acteurs malveillants, privés ou étatiques, peuvent être habiles à découvrirent les failles de systèmes informatiques. Les dernières percées en intelligence artificielle ne peuvent que renforcer nos craintes. Il est illusoire de penser qu'une porte dérobée pour personne autorisée ne puisse être éventuellement exploitée par une personne non autorisée. L'introduction de toute vulnérabilité doit être écartée. Ces dispositions de C-22 sont dangereuses et inacceptables.

CONCLUSION

À l'instar de nombreux autres groupes, la Ligue des droits et libertés réclame le retrait du projet de loi C-22 sur la base des motifs suivants :

1. La possibilité pour les autorités d'accéder à une vaste gamme de renseignements personnels (RRA) auprès de tout fournisseur de service à la population et ce, sur la base de simples motifs raisonnables de *soupçonner* qu'une infraction à n'importe quelle loi fédérale a été ou sera commise;
2. L'immunité civile et pénale en cas de fourniture volontaire de renseignements;
3. L'élargissement excessif des pouvoirs permettant aux policiers de passer outre l'autorisation judiciaire sur la base de la notion de « situation d'urgence », laissée à leur appréciation;
4. L'absence de balises dans l'autorisation d'utilisation par les policiers de renseignements accessibles au public; et l'absence de définition de ce qu'est un tel renseignement;
5. L'utilisation de la norme restreinte du motif raisonnable de soupçonner appliquée aux échanges de renseignements avec des États et entités étrangères;
6. L'accès facilité des entités et autorités étrangères aux données des Canadien·nes, notamment dans la perspective de la ratification du Deuxième protocole additionnel à la Convention de Budapest sur la cybercriminalité et un accord bilatéral avec les États-Unis en vertu du Cloud Act;
7. Le pouvoir d'obliger arbitrairement une quantité innombrable de fournisseurs de service auxquels la population a recours à devenir des instruments à la disposition de l'État pour l'obtention d'information sur leurs client·es;
8. L'obligation faite à des fournisseurs de services de retenir des données très sensibles sur des citoyen·nes afin de les rendre accessibles au SCRS dans le plus grand secret;
9. L'obligation faite à des fournisseurs de service d'installer des portes dérobées mettant les données des citoyen·nes à risque de piratage.

Le projet de loi C-22 accorde aux forces de l'ordre des pouvoirs exorbitants de fouille et de surveillance qui ne sont ni nécessaires, ni raisonnables, ni proportionnés, et met en place une pernicieuse architecture de surveillance représentant de graves atteintes à la vie privée.