BIBLIOTHÈQUE DU PARLEMENT
LIBRARY OF PARLIAMENT

VERSION PRÉLIMINAIRE

NON RÉVISÉE

Ce résumé législatif est offert uniquement en format PDF sous forme de version préliminaire non révisée.

Si le projet de loi reçoit la sanction royale, cette version sera remplacée par une version finale accessible en formats HTML et PDF.

Résumé législatif

PROJET DE LOI C-22 : LOI CONCERNANT L'ACCÈS LÉGAL

45-1-C22-F

Le 7 octobre 2026

Révisée par Sabrina Charland et Anne-Marie Therrien-Tremblay

Services de bibliothèque et de recherche

VERSION PRÉLIMINAIRE
NON RÉVISÉE

ATTRIBUTION

Le 7 octobre 2026	Sabrina Charland et Anne-Marie Therrien-Tremblay
Le 17 mars 2026	Joey Arseneault-Watters, Sabrina Charland, Alexsandra Ferland et Anne-Marie Therrien-Tremblay

À PROPOS DE CETTE PUBLICATION

Les résumés législatifs de la Bibliothèque du Parlement résument des projets de loi à l'étude au Parlement et en exposent le contexte de façon objective et impartiale. Ils sont préparés par les Services de bibliothèque et de recherche, qui effectuent des recherches pour les parlementaires, les comités du Sénat et de la Chambre des communes ainsi que les parlementaires, et leur fournissent de l'information et des analyses. Les résumés législatifs sont mis à jour au besoin pour tenir compte des amendements apportés aux projets de loi au cours du processus législatif.

Par souci de clarté, les propositions législatives du projet de loi décrit dans le présent résumé législatif sont énoncées comme si elles avaient déjà été adoptées ou étaient déjà en vigueur. Il convient cependant de souligner, qu'un projet de loi peut faire l'objet d'amendements au cours de son examen par le Sénat et la Chambre des communes, et qu'il est sans effet avant d'avoir été adopté par les deux Chambres du Parlement, d'avoir reçu la sanction royale et d'être entré en vigueur.

Dans ce résumé législatif de la Bibliothèque du Parlement, tout changement d'importance depuis la publication précédente est signalé en **caractères gras**.

© Bibliothèque du Parlement, Ottawa, Canada, 2026

Résumé législatif du projet de loi C-22
(Version préliminaire)

45-1-C22-F

This publication is also available in English.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

TABLE DES MATIÈRES

1 CONTEXTE 1

2 DESCRIPTION ET ANALYSE 3

2.1 Partie 1 : Accès opportun aux données et aux renseignements (art. 2 à 40 du projet de loi C-22) 3
2.1.1 Examen des données informatiques saisies en vertu d'un mandat 4
2.1.2 Renseignements relatifs à l'abonné 5
2.1.3 Ordre de confirmer la fourniture de services 5
2.1.4 Ordonnance de communication : renseignements relatifs à l'abonné 8
2.1.5 Demande de communication : entité étrangère 8
2.1.6 Urgence de la situation 9
2.1.7 *Loi sur l'entraide juridique en matière criminelle* 10
2.1.8 *Loi réglementant certaines drogues et autres substances* et *Loi sur le cannabis* 11
2.1.9 Entrée en vigueur 12

2.2 Partie 2 : Loi sur le soutien en matière d'accès à de l'information (art. 41 à 47 du projet de loi C-22) 12
2.2.1 Obligations réglementaires des fournisseurs principaux 13
2.2.2 Obligations par arrêtés ministériels 14
2.2.3 Obligations d'assistance et de confidentialité 15
2.2.4 Exécution et contrôle d'application 16
2.2.5 Sanctions administratives pécuniaires et infractions 17
2.2.6 Règlements 18
2.2.7 Rapport annuel 18

2.3 Partie 3 : Examen parlementaire (art. 48 du projet de loi C-22) 19
2.3.1 Examen parlementaire 19

VERSION PRÉLIMINAIRE
NON RÉVISÉE

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-22 : LOI CONCERNANT L'ACCÈS LÉGAL

1 CONTEXTE

Le 12 mars 2026, l'honorable Gary Anandasangaree, ministre de la Sécurité publique et de la Protection civile (ministre de la Sécurité publique), a déposé le projet de loi C-22, Loi concernant l'accès légal (tire subsidiaire : « Loi de 2026 sur l'accès légal ») [1].

Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a proposé 29 modifications au projet de loi lors de son étude qui s'est terminée le 17 juin 2026 [2]. La Chambre des communes a ensuite adopté avec dissidence le projet de loi à l'étape du rapport ainsi qu'à la troisième lecture le 18 juin 2026, sans modifications additionnelles.

Les modifications résultant des amendements adoptés sont identifiées en caractère gras dans le présent document.

Selon le gouvernement du Canada, l'accès légal fait référence à la capacité des organismes d'application de la loi et des organismes de sécurité et de renseignements « à obtenir légalement certains renseignements ou à intercepter des communications [3] ». L'accès légal est encadré par les lois sur la vie privée et la *Charte canadienne des droits et libertés* (la *Charte*), notamment le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Le gouvernement du Canada identifie deux aspects à l'accès légal :

- les pouvoirs des organismes d'application de la loi et du Service canadien du renseignement de sécurité (SCRS) d'obtenir des renseignements et des données, tels qu'énoncés dans le *Code criminel* et la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS) [4];
- la capacité technique des fournisseurs de services électroniques (FSE) de fournir aux organismes d'application de la loi et au SCRS les renseignements qu'ils sont légalement autorisés à obtenir en vertu de ces pouvoirs [5].

La partie 1 du projet de loi C-22 vise le premier aspect susmentionné de l'accès légal. Notamment, les dispositions de cette partie facilitent l'accès par les organismes d'application de la loi et le SCRS à des renseignements d'une personne abonnée à un service de télécommunication.

La partie 2 du projet de loi vise le second aspect susmentionné de l'accès légal. Les dispositions de cette partie édictent la Loi concernant les obligations des fournisseurs de services électroniques en matière d'accès autorisé à de l'information (titre abrégé : « Loi sur le soutien en matière d'accès autorisé à de l'information » (LSAAI)). Selon cette loi, les FSE pourraient être contraints à développer et à maintenir les capacités techniques nécessaires pour faciliter l'accès aux informations qu'elles détiennent par une personne légalement autorisée à y accéder dans le cadre d'enquêtes criminelles ou en matière de renseignement. Selon le gouvernement du Canada :

> Le Canada est le seul pays du Groupe des cinq [une alliance des services de renseignements de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis], du G7 et de l'Union européenne qui n'a pas de législation pour exiger que les FSE développent et maintiennent des capacités en matière d'accès légal [6].

Le Canada a signé en 2001 et ratifié en 2015 la *Convention sur la cybercriminalité* du Conseil de l'Europe (Convention de Budapest) [7]. En 2023, le Canada a signé le *Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques* [8]. Ce protocole fournit un cadre juridique en matière criminelle pour permettre la divulgation de preuves électroniques par des FSE à un pays étranger et pour renforcer la coopération directe entre les pays et les FSE étrangers. Pour le moment, le Canada n'a pas ratifié le protocole. Le Canada n'est donc pas juridiquement lié par les procédures prévues dans le Protocole.

En 2018, les États-Unis ont adopté la *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) [9]. Cette loi prévoit qu'un FSE faisant affaire aux États-Unis est tenu de divulguer des données de ses utilisateurs directement à un pays étranger pour les fins d'une enquête criminelle [10]. L'application de la loi est sujette à l'obtention d'accords bilatéraux réciproques entre les États-Unis et les pays étrangers. Depuis 2022, les États-Unis et le Canada négocient un accord bilatéral relatif à cette loi [11]. À ce jour, les États-Unis ont conclu un accord avec l'Australie et le Royaume-Uni [12].

Le projet de loi C-22 reprend essentiellement les parties 14 et 15 du projet de loi C-2, Loi concernant certaines mesures liées à la sécurité de la frontière entre le Canada et les États-Unis et d'autres mesures connexes liées à la sécurité (titre abrégé : « Loi visant une sécurité rigoureuse à la frontière »), lequel fut déposé le 3 juin 2025 par le ministre de la Sécurité publique [13]. Certaines dispositions du projet de loi C-22 sont néanmoins différentes de celles des parties 14 et 15 du projet de loi C-2. Notamment, la partie 1 prévoit un champ d'application plus restreint pour les demandes d'information sans autorisation judiciaire. Puis, la partie 2 propose des dispositions différentes pour les arrêtés ministériels visant les FSE en exigeant l'approbation du commissaire au renseignement et en retirant l'obligation de

VERSION PRÉLIMINAIRE
NON RÉVISÉE

consultation du ministre de l'Industrie; elle précise également les pouvoirs d'inspection, l'obligation d'aider, la confidentialité et les considérations de cybersécurité [14]. De plus, contrairement au projet de loi C-2, le projet de loi C-22 prévoit à la partie 3 un examen parlementaire du projet de loi trois ans après son entrée en vigueur.

À l'exception des parties 4, 14 et 15, la majorité des mesures prévues dans le projet de loi C-2 ont par la suite été reprises dans le projet de loi C-12, Loi concernant certaines mesures liées à la sécurité de la frontière canadienne et à l'intégrité du système d'immigration canadien et d'autres mesures connexes liées à la sécurité, lequel a depuis été adopté par le Parlement et sanctionné en mars 2026.

Dans les dernières années, le Parlement a adopté des projets de loi concernant l'accès légal. En particulier, la *Loi sur la protection des Canadiens contre la cybercriminalité* [15], adoptée en 2014, permet notamment aux services chargés de l'application de la loi d'ordonner ou d'obtenir une ordonnance judiciaire en vue de la conservation des preuves électroniques et instaure de nouvelles ordonnances judiciaires permettant d'obtenir des données relatives à la transmission de communications ou des données servant à localiser un objet ou une personne. Bien que la *Loi de 2017 sur la sécurité nationale* [16], adoptée en 2019, ne visait pas directement l'accès, elle a, entre autres, réformé le régime de partage de l'information et les règles sur la collecte et l'utilisation des ensembles de données en matière de sécurité nationale.

2 DESCRIPTION ET ANALYSE

Le projet de loi C-22 compte 48 articles et est divisé en trois parties. La partie 1 apporte des modifications à plusieurs lois, la partie 2 édicte la LSAAI, tandis que la partie 3 prévoit l'examen parlementaire des parties 1 et 2. Ce résumé législatif présente les principales dispositions du projet de loi, sans examiner chaque article.

2.1 PARTIE 1 : ACCÈS OPPORTUN AUX DONNÉES ET AUX RENSEIGNEMENTS (ART. 2 À 40 DU PROJET DE LOI C-22)

La partie 1 du projet de loi C-22 modifie plusieurs lois canadiennes, dont le *Code criminel* et la Loi sur le SCRS, en ce qui concerne la collecte de renseignements et les pouvoirs d'accès légal des organismes d'application de la loi et du SCRS. Les principaux éléments de la partie 14 du projet de loi C-2 se retrouvent dans le projet de loi C-22, mais certaines dispositions de ce dernier ont une portée différente.

D'après le gouvernement du Canada, dans le but de donner suite aux arrêts de la Cour suprême du Canada (CSC) dans les affaires *R. c. Spencer* (2014) et *R. c. Bykovets* (2024), selon lesquels une autorisation légale est nécessaire pour

VERSION PRÉLIMINAIRE
NON RÉVISÉE

obtenir des renseignements de base, la partie 1 du projet de loi C-22 donne aux organismes d'application de la loi deux « nouveaux outils pour enquêter [17] ». Il s'agit de (i) l'ordre de confirmer la fourniture de services que le projet de loi C-22 met à la disposition des organismes d'application de la loi et du SCRS au moyen de modifications, respectivement, au *Code criminel* et à la Loi sur le SCRS, et de (ii) l'ordonnance de communication des renseignements relatifs à l'abonné. Outre ces outils, le projet de loi C-22 modifie le *Code criminel* de manière à prévoir l'examen des données informatiques saisies en vertu d'un mandat. Il établit aussi un mécanisme pour demander à une entité étrangère de communiquer des renseignements ainsi que des règles pour la saisie de renseignements numériques sans mandat en cas d'urgence.

2.1.1 Examen des données informatiques saisies en vertu d'un mandat

Pour examiner des données informatiques, les organismes d'application de la loi peuvent demander, aux termes de l'article 487 du *Code criminel*, un mandat de perquisition qui donne le pouvoir d'entrer dans des lieux privés et de saisir des biens. Dans l'arrêt *R. c. Vu* (2013) [18], la CSC a déterminé que les policiers devaient obtenir des tribunaux une autorisation expresse de fouiller un ordinateur, même s'ils avaient déjà un mandat valide de perquisition des lieux. En pratique, cela signifie souvent deux étapes, voire deux mandats.

L'article 3 du projet de loi C-22 modifie l'article 487 du *Code criminel* de manière à permettre à un juge d'autoriser, dans le mandat de perquisition qu'il décerne, l'examen des données informatiques saisies en vertu du mandat ou contenues dans un ordinateur saisi en vertu du mandat (nouveau par. 487(2.3)). Il permet aussi à un juge de décerner un mandat qui autorise l'examen des données contenues dans un ordinateur qui est déjà en la possession des organismes d'application de la loi (nouveau par. 487(2.4)). Dans les deux cas, le juge doit être convaincu qu'il existe des motifs raisonnables de croire [19] que les données informatiques fourniront une preuve d'une infraction.

Le projet de loi C-22 établit des conditions pour l'examen des données informatiques effectué au titre d'un mandat. Plus précisément, selon le nouveau paragraphe 487(2.5), l'examen peut être assorti des conditions que le juge estime indiquées pour que l'examen soit raisonnable. Ces dispositions sont différentes dans le projet de loi C-2, qui permet à un juge d'imposer des conditions précises comme, par exemple, exiger que l'examen soit limité à une catégorie particulière de données informatiques et que l'extraction des données soit effectuée par une personne qui ne participe autrement pas à l'enquête.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.2 Renseignements relatifs à l'abonné

À l'heure actuelle, le *Code criminel* ne définit pas le terme « renseignements relatifs à l'abonné ». Dans l'arrêt *R. c. Spencer*, rendu en 2014, la CSC indique que les renseignements relatifs à l'abonné qui utilise une adresse de protocole Internet (IP) englobent « son nom, son adresse et son numéro de téléphone[20] ». Dans l'arrêt *R. c. Bykovets*, rendu en 2024, la CSC définit le terme comme « les nom, adresse et coordonnées – associés à l'adresse [IP] d'une personne[21] ». Dans *R. c. Spencer*, la CSC établit que les renseignements relatifs à l'abonné s'accompagnent d'une attente raisonnable en matière de respect de la vie privée et qu'une demande faite par les organismes d'application de la loi pour obtenir ces renseignements constitue une « fouille » selon l'article 8 de la *Charte*, qui protège contre les fouilles, les perquisitions ou les saisies abusives. La CSC est arrivée à la même conclusion en ce qui concerne les adresses IP dans l'arrêt *R. c. Bykovets*.

L'article 4 du projet de loi C-22 contient une définition des renseignements relatifs à l'abonné qui a une portée plus large que celle donnée par la CSC et qui englobe le nom, l'adresse, le numéro de téléphone et l'adresse de courriel d'un client d'« une personne fournissant des services au public » ou d'un abonné aux services fournis par une telle personne. Elle comprend aussi le pseudonyme de l'abonné, l'identifiant qui lui a été attribué, comme un numéro de compte, et les « renseignements relatifs aux services fournis à l'abonné », notamment les types de services fournis, la durée de l'abonnement et les renseignements qui identifient les dispositifs et l'équipement utilisés par l'abonné.

Le projet de loi C-22 ne définit pas l'expression « une personne fournissant des services au public ». Elle pourrait être interprétée de manière générale comme toute personne qui offre des services au public et qui peut détenir des données utiles à une enquête de la police. Par exemple, il pourrait s'agir de fournisseurs de services Internet ainsi que de tiers qui offrent des services à des clients ayant des adresses IP, comme des plateformes de médias sociaux, des sites de commerce en ligne, des fournisseurs de services infonuagiques et d'autres entreprises.

2.1.3 Ordre de confirmer la fourniture de services

L'article 5 du projet de loi C-22 modifie le *Code criminel* de manière à permettre aux organismes d'application de la loi d'ordonner à un fournisseur de services de télécommunication de confirmer s'il fournit ou s'il a fourni des services de télécommunication à un abonné, à un client, à un compte ou à un identifiant. L'article 31 du projet de loi C-22 modifie la Loi sur le SCRS afin de permettre au SCRS de donner de tels ordres à des fournisseurs de services de télécommunication.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Le projet de loi C-22 établit des conditions relativement à l'« ordre de confirmer la fourniture de services ». À l'article 5 du projet de loi C-22, le nouveau paragraphe 487.0121(2) du *Code criminel* stipule que l'agent de la paix ou le fonctionnaire public (agent de la paix) ne donne l'ordre que « s'il a des motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise et que la confirmation visée par l'ordre sera utile à l'enquête[22]. L'article 31 du projet de loi C-22 crée le nouveau paragraphe 20.22(1) de la Loi sur le SCRS afin de permettre au SCRS de donner des ordres de confirmer la fourniture de services dans l'exercice de fonctions liées à des « activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada » (art. 12 de la Loi sur le SCRS) ou dans le cadre de la collecte de renseignements sur un État étranger ou une personne étrangère (art. 16 de la Loi sur le SCRS). **À l'étape de l'étude en comité, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a clarifié que la confirmation de la demande de service porte sur des services de télécommunications spécifiquement, et non sur tout type de services en général.**

Contrairement à l'« ordre de fournir des renseignements » du projet de loi C-2, qui peut viser toute « personne fournissant des services au public », l'« ordre de confirmer la fourniture de services » du projet de loi C-22 vise uniquement les fournisseurs de services de télécommunication. Le projet de loi C-22 modifie le *Code criminel* et la Loi sur le SCRS afin de préciser que le terme « fournisseur de services de télécommunication » s'entend au sens de la *Loi sur les télécommunications*[23]. De plus, l'ordre de fournir des renseignements prévu dans le projet de loi C-2 permet aux organismes d'application de la loi et au SCRS de demander davantage de renseignements que le projet de loi C-22, notamment de demander si des services sont fournis et si certains renseignements sont détenus. En revanche, le projet de loi C-22 permet uniquement aux organismes d'application de la loi et au SCRS d'ordonner aux fournisseurs de services de télécommunication de confirmer s'ils fournissent un service.

De plus, le projet de loi C-22 ajoute le paragraphe 487.0121(3) au *Code criminel* et le paragraphe 20.22(2) à la Loi sur le SCRS pour préciser que l'ordre de confirmer la fourniture de services ne peut pas être donné si la confirmation révèle des informations médicales ou des informations protégées par le secret professionnel de l'avocat. Ces mesures de protection ne figurent pas dans les dispositions du projet de loi C-2 relatives à l'ordre de fournir des renseignements.

Dans le projet de loi C-22, le nouveau paragraphe 487.0121(5) du *Code criminel* et le nouveau paragraphe 20.22(3) de la Loi sur le SCRS indiquent que le fournisseur de services de télécommunication doit disposer d'au moins 24 heures pour confirmer le service. De plus, selon les modifications apportées au *Code criminel* et à la Loi sur le SCRS, l'ordre peut être assorti d'une interdiction de divulgation. Les modifications

VERSION PRÉLIMINAIRE
NON RÉVISÉE

à la Loi sur le SCRS ne comportent aucune autre exigence concernant le recours à l'interdiction de divulgation par le SCRS, mais le nouveau paragraphe 487.0121(6) du *Code criminel* indique que l'agent de la paix ne peut imposer une condition de ce genre pour une période d'au plus un an « que s'il a des motifs raisonnables de croire que la divulgation, pendant la période visée, compromettrait le déroulement de l'enquête ».

Le projet de loi C-22 ajoute les paragraphes 487.0121(8) à 487.0121(11) au *Code criminel* afin d'établir un processus de révision qui permet au fournisseur de services de télécommunication de demander par écrit à un juge de modifier ou de révoquer l'ordre de confirmer la fourniture de services. Il ajoute aussi l'article 20.23 à la Loi sur le SCRS pour établir un processus de révision semblable.

En outre, le nouvel article 20.24 de la Loi sur le SCRS crée un processus qui permet au SCRS de demander à un juge d'ordonner au fournisseur de services de télécommunication de donner la confirmation. Les articles 32 à 34 du projet de loi C-22 modifient les dispositions de la Loi sur le SCRS relatives à la modification ou à la révocation des ordonnances de manière à tenir compte de la modification ou de la révocation des ordres de confirmer la fourniture de services et des ordonnances rendues en vertu de l'article 20.24 ainsi que d'autres modifications apportées à la loi. Le projet de loi C-2 contient des dispositions semblables. **Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a modifié l'alinéa 28(b.2) de la Loi sur le SCRS afin de clarifier le pouvoir réglementaire applicable aux nouvelles dispositions. Plutôt que d'énumérer les différentes catégories de demandes de modification ou de révocation pouvant être présentées relativement aux nouveaux ordres et ordonnances, la disposition renvoie désormais aux demandes présentées en vertu des articles 20.23 et 20.5.**

De plus, le projet de loi C-22 ajoute le nouveau paragraphe 487.0121(11) au *Code criminel* et le nouveau paragraphe 20.25(1) à la Loi sur le SCRS afin de préciser que, si un fournisseur de services de télécommunication veut fournir volontairement la confirmation, il n'est pas nécessaire d'obtenir un pouvoir additionnel, comme une ordonnance d'un tribunal. Le projet de loi C-2 ne contient pas de disposition équivalente. L'article 11 du projet de loi C-22 apporte des précisions semblables pour les ordres de confirmer la fourniture de services ainsi que pour les ordonnances de communication et les mandats et confirme, dans le nouveau paragraphe 487.0195(4) du *Code criminel*, que les organismes d'application de la loi n'ont pas besoin d'une ordonnance pour obtenir des renseignements auxquels le public a déjà accès. L'article 164 du projet de loi C-2 contient des dispositions semblables.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.4 Ordonnance de communication : renseignements relatifs à l'abonné

À l'heure actuelle, les organismes d'application de la loi peuvent présenter une demande d'ordonnance générale de communication à un tribunal pour obtenir des renseignements relatifs à l'abonné[24]. L'article 6 du projet de loi C-22 prévoit des ordonnances de communication visant précisément les renseignements relatifs à l'abonné dans le nouvel article 487.0142 du *Code criminel*. Cette ordonnance de production permet aux organismes d'application de la loi d'exiger, sur demande *ex parte* présentée à un juge[25], qu'un fournisseur de service communique un document **comprenant des renseignements relatifs à l'abonné.**

Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a modifié l'article 6 afin que les renseignements qui peuvent être communiqués soient explicitement limités aux catégories identifiées dans la nouvelle définition de « renseignements relatifs à l'abonné » établie par l'article 487.011 du *Code criminel*. L'article 6, tel que modifié à l'étape de l'étude en comité, clarifie que les renseignements demandés doivent (1) se limiter spécifiquement à ceux identifiées dans l'ordonnance, (2) se rapporter à des données précisées dans l'ordonnance, et (3) se trouver en la possession ou à la disposition du fournisseur au moment de la réception de l'ordonnance.

L'agent de la paix doit faire une dénonciation sous serment selon la formule 5.004 afin que le juge rende l'ordonnance s'il existe « des motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise et que les renseignements seront utiles à l'enquête. En comparaison, la norme plus contraignante des « motifs raisonnables de croire » est exigée pour qu'un juge rende une ordonnance générale de communication.

L'ordonnance de communication des renseignements relatifs à l'abonné établie par l'article 6 du projet de loi C-22 s'applique à toute « personne fournissant des services publics », ce qui lui donne une plus grande portée que l'ordre de confirmer la fourniture de services prévu à l'article 5 du projet de loi, qui s'applique uniquement aux fournisseurs de services de télécommunication.

2.1.5 Demande de communication : entité étrangère

L'article 7 du projet de loi C-22 modifie le *Code criminel* par adjonction du nouvel article 487.018, qui permet aux organismes d'application de la loi de présenter des demandes de communication à des fournisseurs de services de télécommunication étrangers. D'après le gouvernement du Canada, il n'existe à l'heure actuelle « aucun outil particulier qui permette aux organismes canadiens d'application de la loi de demander aux entités étrangères des renseignements sur les personnes abonnées ou des données de transmission conservés à l'étranger[26] ».

VERSION PRÉLIMINAIRE
NON RÉVISÉE

L'article 7 du projet de loi C-22 permet à un agent de la paix, au moyen d'une demande *ex parte*, de demander « à une entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication » de communiquer un document comportant les données de transmission, au sens de l'article 487.011 du *Code criminel*, ou les renseignements relatifs à l'abonné, au sens de l'article 2 du projet de loi C-22. Le juge peut autoriser la demande s'il est convaincu qu'il existe des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise, et que les renseignements sont en possession de l'entité étrangère et seront utiles à l'enquête.

Les dispositions régissant les demandes de communication soumises à des entités étrangères prévues dans le projet de loi C-22 sont semblables à celles contenues dans le projet de loi C-2. Toutefois, dans le projet de loi C-2, la demande de communication s'applique à « une entité étrangère qui fournit au public des services de télécommunication », sans inclure les entités qui fournissent des services « à l'aide d'un moyen de télécommunication » comme le fait el projet de loi C-22.

2.1.6 Urgence de la situation

À l'heure actuelle, un agent de la paix peut effectuer une fouille dans un bâtiment, un contenant ou un lieu ou utiliser un dispositif de localisation (pour surveiller le lieu d'une opération ou les déplacements d'une chose) sans ordonnance d'un tribunal si l'urgence de la situation rend difficile son obtention[27]. Il y a notamment urgence dans les cas où tout retard dans l'obtention d'une ordonnance risque d'entraîner la perte de preuves ou de mettre en danger quelqu'un. Toutefois, selon le gouvernement du Canada, les organismes d'application de la loi ne disposent pas en ce moment « d'une capacité clairement établie de traiter les renseignements qui doivent leur être fournis au titre de la loi sans avoir à obtenir l'autorisation d'un tribunal[28] ».

L'article 14 du projet de loi C-22 modifie l'article 487.11 du *Code criminel* afin d'élargir la capacité des organismes d'application de la loi d'effectuer une fouille sans mandat dans les situations d'urgence, notamment pour obtenir les données de localisation d'une personne au moyen d'un dispositif de localisation (par. 492.1(2) du *Code criminel* relatif au mandat pour un dispositif de localisation) et pour obtenir les données de transmission au moyen d'un enregistreur de données de transmission (art. 492.2 du *Code criminel* relatif au mandat pour les données de transmission). En outre, dans les situations où il y a urgence, le nouvel alinéa 487.11b) permettrait aux organismes d'application de la loi de saisir, sans ordonnance du tribunal :

- les renseignements relatifs à l'abonné visés par les nouvelles dispositions du projet de loi C-22 prévoyant les ordonnances de communication des renseignements relatifs à l'abonné (par. 487.0142(1) du *Code criminel*);

VERSION PRÉLIMINAIRE
NON RÉVISÉE

- les données de transmission obtenues au moyen d'une ordonnance rendue en vertu du paragraphe 487.016(1) du *Code criminel*;
- les données de localisation obtenues au moyen d'une ordonnance rendue en vertu du paragraphe 487.017(1) du *Code criminel*.

L'article 19 du projet de loi C-22 modifie l'article 492.1 du *Code criminel* de manière à élargir la portée des mandats applicables aux données de localisation afin que les agents de la paix puissent obtenir les données de localisation qui concernent le lieu d'une chose (inconnue au moment de la délivrance du mandat) qu'une personne utilise, porte ou transporte (nouveau par. 492.1(2.1)).

L'article 20 du projet de loi C-22 élargit aussi la portée de l'article 492.2 du *Code criminel* de manière à autoriser les agents de la paix à obtenir les données de transmission qui concernent un moyen de télécommunication inconnu au moment où le mandat est délivré. Le projet de loi C-22 ajoute le paragraphe 492.2(2.1) au *Code criminel* afin de permettre à un juge d'inclure les conditions qu'il « estime indiquées, notamment quant à la protection des intérêts de toute personne » lorsqu'il délivre un mandat visant les données de transmission. Cette disposition ne figure pas dans le projet de loi C-2.

Les dispositions relatives à l'urgence du projet de loi C-22 sont semblables à celles du projet de loi C-2.

2.1.7 *Loi sur l'entraide juridique en matière criminelle*

L'article 29 du projet de loi C-22 apporte des modifications à la *Loi sur l'entraide juridique en matière criminelle* (LEJMC)[29]. Cette loi prévoit la mise en œuvre de traités d'entraide juridique en matière criminelle et confère au Canada le pouvoir légal d'obtenir des ordonnances judiciaires au nom des pays qui sont parties à ces accords. Les demandes d'entraide présentées au titre de la LEJMC peuvent notamment concerner des enquêtes étrangères, des mandats d'arrestation, des ordonnances de communication, l'exécution de perquisitions, de fouilles ou de saisies, le transfert de personnes condamnées et la confiscation de biens entre le Canada et des pays partenaires.

Le projet de loi C-22 ajoute le nouvel article 22.07 à la LEJMC sous « Exécution de décisions étrangères de communication ». Ce nouvel article permet aux autorités canadiennes d'exécuter la décision d'un pays partenaire nécessitant la communication de données électroniques précises conservées au Canada, à savoir des données de transmission ou des renseignements relatifs à l'abonné. Le nouveau paragraphe 22.07(1) de la LEJMC prévoit que le ministre de la Justice peut autoriser une « autorité compétente » à exécuter la décision lorsqu'une demande d'entraide est présentée.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Le terme « autorité compétente » est défini dans la LEJMC comme « [l]e procureur général du Canada, le procureur général d'une province ainsi que toute personne ou tout organisme chargé au Canada de la recherche ou de la poursuite des infractions [30] ».

Selon le nouveau paragraphe 22.07(2) de la LEJMC, l'autorité compétente doit d'abord présenter à un juge une requête *ex parte* en vue de l'exécution de la décision. Les conditions à respecter pour que le juge rende la décision exécutoire dépendent du type de renseignement demandé (nouveau par. 22.07(3) de la LEJMC). Pour les données de transmission, le juge doit être convaincu que les conditions nécessaires pour rendre une ordonnance de communication des données de transmission, énoncées au paragraphe 487.016(2) du *Code criminel*, sont réunies [31]. Pour les renseignements relatifs à l'abonné, le juge doit être convaincu que les conditions nécessaires pour rendre une ordonnance de communication des renseignements relatifs à l'abonné, énoncées au nouveau paragraphe 487.0142(2) du *Code criminel*, sont réunies.

Les modifications apportées à la LEJMC établissent des délais pour la communication de documents contenant des données de transmission ou des renseignements relatifs à l'abonné (par. 22.07(5) de la LEJMC) et permettent au juge de demander que l'autorité compétente communique les renseignements directement à une personne désignée dans le pays partenaire (al. 22.07(7)a) de la LEJMC), qui doit alors les transmettre au pays partenaire dans les cinq jours suivant la date à laquelle le document a été communiqué (par. 22.07(9) de la LEJMC). Les modifications apportées à la LEJMC comportent aussi des exigences d'établissement de rapport.

De plus, le paragraphe 22.07(10) de la LEJMC renvoie à une infraction punissable par procédure sommaire prévue au *Code criminel* en cas de non-respect de l'ordonnance de communication. En conséquence, la partie coupable d'avoir contrevenu à une ordonnance de communication sans excuse légitime encourt une amende maximale de 250 000 $ et un emprisonnement maximal de deux ans moins un jour, ou l'une de ces peines [32].

Les dispositions régissant les demandes de communication d'entités étrangères prévues dans le projet de loi C-22 sont les mêmes que dans le projet de loi C-2.

2.1.8 *Loi réglementant certaines drogues et autres substances* et *Loi sur le cannabis*

Les articles 37 et 38 du projet de loi modifient, respectivement, la *Loi réglementant certaines drogues et autres substances* [33] et la *Loi sur le cannabis* [34]. Ces modifications visent certaines dispositions du *Code criminel* liées aux données informatiques et d'autres ajouts au *Code criminel*, plus précisément les dispositions régissant le traitement de la preuve électronique selon les mandats de perquisition.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.9 Entrée en vigueur

La partie 1 du projet de loi C-22 entre en vigueur 180 jours après la date de la sanction royale.

2.2 PARTIE 2 : LOI SUR LE SOUTIEN EN MATIÈRE D'ACCÈS À DE L'INFORMATION (ART. 41 À 47 DU PROJET DE LOI C-22)

La partie 2 du projet de loi C-22 comporte six articles. L'article 41 édicte la LSAAI. Les articles 42 à 46 prévoient diverses dispositions connexes et corrélatives, notamment des modifications à la *Loi sur le commissaire au renseignement*, tandis que l'article 47 établit que l'entrée en vigueur de ces dispositions sera fixée par décret. Bien qu'elle s'inspire largement de la partie 15 du projet de loi C-2, Loi visant une sécurité rigoureuse à la frontière, la partie 2 du projet de loi C-22 introduit certaines différences importantes, notamment en matière de surveillance, de transparence et de cadre réglementaire.

Selon le gouvernement du Canada, la LSAAI a pour objet de faciliter l'accès, dans un cadre légal, par des personnes autorisées à l'information détenue par des FSE, notamment dans le contexte d'enquêtes policières ou d'opérations de renseignement (art. 3 de la LSAAI). À cette fin, la LSAAI s'applique aux FSE, définis comme toute personne offrant des services électroniques, notamment afin de permettre la communication, soit à des personnes situées au Canada, soit dans le cadre d'activités commerciales exercées en tout ou en partie au Canada (art. 2 de la LSAAI).

À l'étape de l'étude en comité, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a ajouté la précision que la LSAAI ne modifie pas les pouvoirs d'accès à l'information déjà prévus par d'autres lois fédérales ni les ententes d'assistance existantes. Une précision quant aux limites des obligations pouvant être imposées aux FSE a également été ajoutée. Elle prévoit notamment que la LSAAI ne peut servir à obliger un FSE à déchiffrer une information chiffrée par un utilisateur ou à garantir son déchiffrement, sauf lorsque le chiffrement est fourni par le FSE lui-même et qu'il possède les moyens techniques nécessaires pour déchiffrer l'information (par. 2(2) à 2(4) de la LSAAI).

La LSAAI établit deux mécanismes par lesquels des obligations peuvent être imposées aux FSE : premièrement, par la désignation à titre de fournisseur principal, entraînant des obligations réglementaires; ou deuxièmement, par l'émission d'un arrêté ministériel. La LSAAI prévoit également des obligations générales d'aide et de confidentialité applicables aux FSE, un régime d'inspection et de surveillance, ainsi que des sanctions administratives pécuniaires et des infractions pénales en cas de non-conformité.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.2.1 Obligations réglementaires des fournisseurs principaux

Le gouverneur en conseil peut désigner certaines catégories de FSE comme « fournisseurs principaux » en les inscrivant à l'annexe de la LSAAI (par. 5(1) de la LSAAI), bien qu'aucune catégorie de fournisseur n'y soit présentement inscrite.

Le paragraphe 5(2) de la LSAAI permet au gouverneur en conseil d'établir par règlement les obligations des fournisseurs principaux, notamment en matière de capacités techniques, d'équipement et d'avis à transmettre au ministre de la Sécurité publique. Comparativement au projet de loi C-2, le projet de loi C-22 ajoute à cette liste la possibilité d'exiger la conservation de catégories de métadonnées, y compris les données de transmission définies à l'article 487.011 du *Code criminel*[35], pour une période maximale de **six mois**[36]**.**

Il s'agit par exemple de renseignements techniques liés au moment, à la durée ou à l'acheminement d'une communication, sans pour autant révéler le contenu de la communication.

Le projet de loi C-22 introduit également, au paragraphe 5(3) de la LSAAI, un élément ne se trouvant pas au projet de loi C-2. Ce paragraphe oblige le gouverneur en conseil à tenir compte de plusieurs facteurs au moment de prendre un règlement en vertu du paragraphe 5(2) de la LSAAI, y compris les avantages du règlement pour l'administration de la justice et la sécurité nationale, la capacité des fournisseurs principaux de s'y conformer, les coûts liés à cette conformité, les effets possibles sur les utilisateurs des services, les impacts sur la vie privée et la cybersécurité, ainsi que tout autre facteur jugé pertinent.

Le paragraphe 5(4) de la LSAAI introduit également un élément ne se trouvant pas au projet de loi C-2, en prévoyant des restrictions précises quant à la portée de l'alinéa 5(2)d), notamment pour assurer que les règlements ne puissent obliger les fournisseurs principaux à conserver de l'information révélant le contenu des communications, l'historique de navigation Web ou les activités d'une personne sur les médias sociaux. **Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a par ailleurs ajouté les paragraphes 5(4.1) et 5(6), qui limitent davantage la portée de ce pouvoir réglementaire en exigeant que les catégories de métadonnées visées soient essentielles à certaines fins d'enquête ou de renseignement et en précisant qu'aucun pouvoir d'accès à des renseignements personnels ne peut être créé par règlement.**

Enfin, le paragraphe 5(5) de la LSAAI contient une disposition similaire au paragraphe 5(3) du projet de loi C-2, établissant qu'un fournisseur principal ne soit pas tenu de se conformer à une obligation réglementaire si cela l'obligeait à introduire une vulnérabilité systémique ou à empêcher de corriger une telle

VERSION PRÉLIMINAIRE
NON RÉVISÉE

vulnérabilité dans les protections électroniques du service. D'ailleurs, le projet de loi C-22 prévoit une définition explicite de « vulnérabilité systémique », laquelle désigne toute vulnérabilité dans les protections électroniques d'un service électronique qui crée, **selon des normes techniques internationales reconnues, un risque crédible d'accès non autorisé à de l'information sécurisée**[37]**.**

L'article 6 de la LSAAI permet à un fournisseur principal de demander une exemption temporaire à certaines obligations réglementaires. Le ministre de la Sécurité publique peut l'accorder, sous conditions et pour une durée déterminée, si la demande est justifiée et accompagnée des renseignements requis. Pendant l'examen de la demande, l'obligation ne s'applique pas, et en cas de refus, le Ministre peut accorder un délai précis pour s'y conformer. **L'article 6 a été modifié à l'étape de l'étude en comité, afin de permettre au Ministre d'imposer des conditions relatives à la communication de l'existence ou du contenu d'une exemption temporaire et d'exiger qu'il rende sa décision dans un délai de 90 jours suivant la présentation de la demande, sauf en cas d'entente contraire avec le fournisseur principal.**

2.2.2 Obligations par arrêtés ministériels

Le paragraphe 7(1) de la LSAAI autorise le ministre de la Sécurité publique à imposer, par arrêté, toute obligation pouvant être prévue par règlement en vertu du paragraphe 5(2) et à en fixer la durée. En vertu du projet de loi C-22, l'arrêté n'entre toutefois en vigueur qu'une fois approuvé par le commissaire au renseignement, qui doit fournir une décision écrite à cet effet (par. 7(2) de la LSAAI), une restriction qui n'est pas prévue au projet de loi C-2. **Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a également modifié l'article 7 afin de plafonner à deux ans la période de validité des arrêtés ministériels et d'autoriser l'inclusion de dispositions régissant la communication de leur existence ou de leur contenu.**

Comme prévu au projet de loi C-2, le ministre de la Sécurité publique doit tenir compte d'une série de facteurs pour prendre un arrêté, tels que les avantages pour la justice, la faisabilité, les coûts de conformité, et les impacts sur les usagers du FSE (par. 7(3) de la LSAAI). Le projet de loi C-22 élargit toutefois cette liste en y ajoutant un facteur distinct relatif à la protection de la vie privée et à la cybersécurité (al. 7(3)e) de la LSAAI).

Une indemnité peut être prévue pour compenser les frais de conformité du FSE (par. 7(4) de la LSAAI). Comme pour les obligations réglementaires, un fournisseur peut être exempté si l'obligation crée ou empêche de corriger une « vulnérabilité systémique ».

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Avant de prendre un arrêté au titre du paragraphe 7(1), le ministre de la Sécurité publique doit donner au FSE concerné la possibilité de présenter ses observations (art. 8 de la LSAAI). Contrairement au projet de loi C-2, le projet de loi C-22 n'exige pas que le ministre de la Sécurité publique consulte le ministre de l'Industrie; il prévoit plutôt que tout arrêté soit transmis au commissaire au renseignement afin que ce dernier l'examine et l'approuve conformément à la *Loi sur le commissaire au renseignement* (art. 9 de la LSAAI). **À l'étape de l'étude en comité, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a également modifié l'article 9 de la LSAAI afin d'exiger que les arrêtés approuvés ainsi que les renseignements transmis au commissaire au renseignement soient communiqués à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) pour appuyer l'exercice de son mandat de surveillance [38].**

L'arrêté est valide pour la période précisée, sauf révocation (art. 10 de la LSAAI). **À l'étape de l'étude en comité, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a supprimé les dispositions qui permettaient de prolonger la période de validité d'un arrêté sans nouvel examen par le Commissaire au renseignement du Canada. Le Comité a également retiré l'obligation faite au ministre de la Sécurité publique d'examiner les arrêtés avant leur expiration en vue de déterminer s'il convenait d'en prolonger la validité.** En cas de conflit entre un arrêté et un règlement pris en vertu de l'article 5, l'arrêté prévaut (art. 1**2** de la LSAAI).

2.2.3 Obligations d'assistance et de confidentialité

Les FSE ont l'obligation de fournir, sur demande, toute assistance raisonnable pour évaluer ou tester des dispositifs permettant à une personne autorisée d'accéder à de l'information. Cette demande peut provenir de personnes ayant qualité pour le faire et spécifiquement énumérées à l'article 1**3** de la LSAAI, et doit être respectée dans les délais et les modalités prévus par règlement.

En vertu du projet de loi C-22, la demande d'assistance doit être présentée par le Ministre ou par toute autre personne nommée dans les catégories de demandeur permis [39]. Elle doit aussi être formulée par écrit et préciser son objet ainsi que toute restriction ou condition applicable. Enfin, le projet de loi C-22 prévoit expressément que ces activités d'évaluation ou de mise à l'essai ne peuvent permettre l'accès à des renseignements personnels (art. 1**3** de la LSAAI).

L'article 1**4** de la LSAAI interdit aux FSE et à toute personne agissant en son nom de communiquer diverses informations liées aux arrêtés ministériels, sauf si la LSAAI ou la *Loi sur la preuve au Canada* l'autorise. Ces interdictions reprennent

VERSION PRÉLIMINAIRE
NON RÉVISÉE

essentiellement celles prévues sous le projet de loi C-2, à l'exception de celle visant l'information liée à une vulnérabilité systémique, qui n'est pas prévue dans le projet de loi C-22. **Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a ajouté le nouvel article 15 à la LSAAI afin de permettre à un FSE d'obtenir l'autorisation écrite du ministre de la Sécurité publique de communiquer certains renseignements visés par une interdiction de communication. Le Ministre peut assortir cette autorisation des conditions qu'il estime raisonnables et doit l'accorder lorsque l'information est utile à l'exercice des attributions d'une autorité administrative.**

L'article 16 de la LSAAI établit un régime de confidentialité applicable à l'information obtenue par les personnes désignées dans l'exercice de leurs inspections effectuées en vertu des articles 20 et 21 de la LSAAI, ainsi qu'à l'information obtenue dans un rapport de vérification interne prévu à l'article 23. Ce régime n'est pas prévu dans le projet de loi C-2.

Le droit pour un FSE de contester par contrôle judiciaire un arrêté ou une décision figure à l'article 17 de la LSAAI. Comme c'est le cas à l'article 16 de la LSAAI sous le projet de loi C-2, un préavis écrit d'au moins 15 jours doit être transmis au Ministre; toutefois, le paragraphe 17(2) précise que la Cour fédérale a compétence exclusive pour entendre ces demandes.

L'article 18 de la LSAAI, tel que proposé dans le projet de loi C-22, habilite le gouverneur en conseil à prendre des règlements relatifs à la confidentialité de l'information, à la sécurité des installations et aux exigences applicables au personnel. Ces pouvoirs portent également sur la communication et la protection de l'information visées aux nouveaux articles 1**4** et 16 de la LSAAI, ainsi que sur les exigences concernant l'habilitation de sécurité du personnel et les installations utilisées pour le traitement de l'information faisant l'objet d'une demande d'accès légal. Les pouvoirs réglementaires correspondants prévus à l'article 17 de la LSAAI dans le projet de loi C-2 étaient plus limités.

2.2.4 Exécution et contrôle d'application

Le ministre de la Sécurité publique peut désigner, sous conditions, toute personne chargée de faire respecter la LSAAI. Il lui délivre un certificat attestant cette désignation. La personne désignée doit présenter ce certificat sur demande pour s'identifier dans le cadre de ses fonctions (art. 19 de la LSAAI).

Une personne désignée peut entrer dans tout lieu (sauf une maison d'habitation) pour vérifier la conformité à la LSAAI, sur motifs raisonnables de croire qu'une activité ou des éléments pertinents s'y trouvent. Elle détient le pouvoir d'examiner, de reproduire ou d'emporter tout document ou toutes données électroniques et d'utiliser

VERSION PRÉLIMINAIRE
NON RÉVISÉE

les équipements sur place pour le faire. Le personnel du FSE est alors tenu de lui prêter assistance (art. 20 de la LSAAI). Pour entrer dans une maison d'habitation sans le consentement de l'occupant, un mandat est requis (art. 21 de la LSAAI), et l'usage de la force n'est permis que si le mandat l'autorise et qu'un agent de la paix est présent.

La personne désignée peut aussi ordonner à un FSE de réaliser une vérification interne de ses pratiques, documents et données électroniques à toute fin liée à la vérification du respect ou à la prévention du non-respect de la LSAAI (art. 22 de la LSAAI). Le FSE doit se conformer à la vérification interne et remettre un rapport détaillé de celle-ci (art. 23 de la LSAAI). Si elle a des motifs raisonnables de croire **qu'il y a ou qu'il y aura vraisemblablement une contravention à une disposition de la LSAAI**, la personne désignée peut demander au FSE de cesser l'activité en cause et de prendre les mesures nécessaires par l'imposition d'un ordre de conformité (art. 24 de la LSAAI). Le FSE doit respecter cet ordre et en informer la personne désignée une fois qu'il s'y est conformé (art. 25 de la LSAAI). **Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a ajouté aux articles 24 et 25 de la LSAAI une exception permettant à un FSE de ne pas se conformer à un ordre de conformité lorsque celui-ci l'obligerait à introduire une vulnérabilité systémique ou l'empêcherait d'en corriger une.**

Le FSE peut demander une révision de l'ordre de conformité auprès du Ministre, mais l'ordre demeure en vigueur pendant l'examen, sauf décision contraire. Si aucune décision n'est rendue dans les 90 jours de la demande de révision par le FSE, l'ordre est réputé être confirmé (art. 26 et 27 de la LSAAI). **Un amendement adopté par le Comité a ajouté à l'article 27 des obligations visant à informer l'OSSNR des ordres de conformité délivrés, des demandes de révision présentées à leur égard et des décisions rendues par le ministre de la Sécurité publique, afin de soutenir l'exercice du mandat de surveillance de cet organisme.**

2.2.5 Sanctions administratives pécuniaires et infractions

La LSAAI prévoit des sanctions administratives pécuniaires (art. 28 à 31) et des infractions pénales (art. 41 à 46) qui visent toutes deux à assurer le respect de la loi, mais diffèrent par leur nature et leurs conséquences.

Les sanctions administratives pécuniaires ne visent pas à punir, mais à favoriser le respect de la LSAAI (art. 28 de la LSAAI) et elles s'appliquent en cas de violation de certaines dispositions légales ou réglementaires. Elles peuvent entraîner des amendes allant jusqu'à 50 000 $ pour une personne physique et jusqu'à 250 000 $ pour une entité, avec une violation distincte comptée par jour (art. 29 de la LSAAI).

Les mêmes types de contraventions, sur déclaration de culpabilité par procédure sommaire, peuvent entraîner des infractions de nature pénale et mener à des amendes

VERSION PRÉLIMINAIRE
NON RÉVISÉE

plus élevées, soit jusqu'à 100 000 $ pour une personne physique et 500 000 $ pour une entité. Celles-ci sont également calculées comme une violation distincte par jour (art. 41 de la LSAAI).

Dans les deux cas, une défense est possible si l'auteur prouve avoir pris toutes les précautions voulues (par. 29(4) et 41(4) de la LSAAI). Dans les deux cas aussi, la violation ou l'infraction peut être prouvée par les actes d'un employé ou d'un mandataire, même si ce dernier n'est pas identifié (art. 30 et 42 de la LSAAI), et les dirigeants ou mandataires d'une entité peuvent être tenus personnellement responsables s'ils ont participé à la violation ou à l'infraction (art. 31 et 43 de la LSAAI).

Enfin, d'autres infractions spécifiques sont prévues pour obstruction (art. 44 de la LSAAI) ou fausses déclarations (art. 45 de la LSAAI), avec des amendes distinctes (art. 46 de la LSAAI).

2.2.6 Règlements

Le paragraphe 47(1) de la LSAAI autorise le gouverneur en conseil à prendre des règlements concernant divers aspects de la mise en œuvre de la LSAAI, notamment les frais payables aux FSE pour l'assistance fournie, la tenue de registres et la préparation de rapports, le sens à donner à certains termes de la LSAAI, ainsi que les modalités applicables aux ordres et aux rapports prévus par celle-ci.

Le paragraphe 47(2) de la LSAAI impose au ministre de la Sécurité publique d'effectuer un examen des règlements tous les cinq ans à compter de la date de l'adoption du premier règlement. Le paragraphe 47(3) exige la publication d'un avis public avant l'adoption du premier règlement et lors de chaque examen, afin de recueillir les observations des procureurs généraux du Canada et de chaque province, des fournisseurs principaux et des FSE visés par un arrêté.

Enfin, l'article 48 de la LSAAI précise que les règlements peuvent établir différentes catégories de FSE et les traiter différemment selon leurs services ou la taille de leur clientèle au Canada.

2.2.7 Rapport annuel

Comparativement au projet de loi C-2, le projet de loi C-22 prévoit, à l'article 49 à la LSAAI, l'obligation pour le Ministre de publier un rapport annuel sur l'application de la LSAAI. Ce rapport doit indiquer le nombre d'arrêtés pris ou refusés par le commissaire au renseignement, les catégories de FSE visées, les obligations imposées, les mesures de conformité appliquées et les demandes d'assistance prévues à l'article 14 de la LSAAI. Une version caviardée doit être rendue publique dans les 60 jours, tandis que la version intégrale doit être transmise au Comité des

VERSION PRÉLIMINAIRE
NON RÉVISÉE

parlementaires sur la sécurité nationale et le renseignement ainsi qu'à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.

2.3 PARTIE 3 : EXAMEN PARLEMENTAIRE (ART. 48 DU PROJET DE LOI C-22)

2.3.1 Examen parlementaire

La partie 3 du projet de loi C-22 prévoit un examen parlementaire du projet de loi trois ans après son entrée en vigueur. Selon un document d'information du gouvernement du Canada, cet examen parlementaire contribuerait à accroître davantage la transparence[40].

NOTES

1. Projet de loi C-22, Loi concernant l'accès légal, 45e législature, 1re session.
2. Chambre des communes, Comité permanent de la sécurité publique et nationale, *Projet de loi C-22, Loi concernant l'accès légal*, cinquième rapport, juin 2026.
3. Gouvernement du Canada, *Accès légal*.
4. *Code criminel*, L.R.C. 1985, ch. C-46; et *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23.
5. Gouvernement du Canada, *Accès légal*.
6. *Ibid*.
7. Conseil de l'Europe, *Convention sur la cybercriminalité*, 23 novembre 2001.
8. Conseil de l'Europe, *Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques*, 12 mai 2022.
9. États-Unis, *Consolidated Appropriations Act, 2018*, Public Law 115-141, 155e Congrès, 132 Stat. 348.
10. Pour plus d'information, voir notamment Michael Fekete et John Salloum, « La souveraineté des données au regard du CLOUD Act : retour vers le futur? », *Osler*, 7 octobre 2025; et Association du Barreau canadien, « Comment aborder la question des divulgations de données numériques par le Canada aux États-Unis », *ABC National*, 31 janvier 2025.
11. États-Unis, Département de la Justice, *CLOUD Act Resources*.
12. *Ibid*.
13. Projet de loi C-2, Loi concernant certaines mesures liées à la sécurité de la frontière entre le Canada et les États-Unis et d'autres mesures connexes liées à la sécurité, 45e législature, 1re session.
14. Sécurité publique Canada, *Loi sur le soutien en matière d'accès autorisé à de l'information (projet de loi C-22 – partie 2)*, document d'information.
15. *Loi sur la protection des Canadiens contre la cybercriminalité*, L.C. 2014, ch. 31.
16. *Loi de 2017 sur la sécurité nationale*, L.C. 2019, ch. 13.
17. Ministère de la Justice Canada, *Modifications proposées aux lois sur l'accès aux renseignements en temps opportun (Projet de loi C-22 – Partie 1)*, document d'information.
18. *R. c. Vu*, 2013 CSC 60 (CanLII).

VERSION PRÉLIMINAIRE
NON RÉVISÉE

19. Le critère des « motifs raisonnables de croire » est le seuil du *Code criminel* qui autorise l'obtention d'un mandat de perquisition au Canada. Dans l'arrêt *R. c. Storrey*, [1990] 1 R.C.S. 241, la Cour suprême du Canada explique que quiconque exerce un pouvoir reposant sur le « motif raisonnable de croire » doit avoir subjectivement « des motifs raisonnables et probables » de l'exercer. Ces motifs doivent « être objectivement justifiables ».

20. *R. c. Spencer*, 2014 CSC 43, par. 11.

21. Selon l'arrêt rendu par la Cour suprême du Canada dans l'affaire *R. c. Bykovets*, une adresse de protocole Internet (IP) est

> un numéro d'identification unique. De telles adresses identifient une activité connectée à Internet et permettent le transfert d'information d'une source à une autre. Elles sont nécessaires pour accéder à Internet. Une adresse IP identifie la source de toute activité en ligne et relie cette activité (au moyen d'un modem) à un endroit donné. De plus, le fournisseur de services Internet (FSI) conserve les renseignements relatifs à l'abonné qui se rattachent à chaque adresse IP.

22. Au paragraphe 75 de l'arrêt *R. c. Kang-Brown*, 2008 CSC 18, la Cour suprême du Canada donne la définition suivante de « motifs raisonnables de soupçonner » :

> Les « soupçons » sont une impression que l'individu ciblé se livre à une activité criminelle. Les soupçons « raisonnables » sont plus que de simples soupçons, mais ils ne correspondent pas à une croyance fondée sur des motifs raisonnables et probables.

Au paragraphe 27 de l'arrêt *R. c. Chehil*, 2013 CSC 49, la Cour suprême du Canada indique que

> bien que les motifs raisonnables de soupçonner, d'une part, et les motifs raisonnables et probables de croire, d'autre part, soient semblables en ce sens qu'ils doivent, dans les deux cas, être fondés sur des faits objectifs, les premiers constituent une norme moins rigoureuse, puisqu'ils évoquent la possibilité – plutôt que la probabilité – raisonnable d'un crime.

23. Selon le par. 2(1) de la *Loi sur les télécommunications*, un « fournisseur de services de télécommunication » est une « personne qui fournit des services de télécommunication de base, y compris au moyen d'un appareil de transmission exclu ». *Loi sur les télécommunications*, L.C. 1993, ch. 38, par. 2(1).

24. *Code criminel*, L.R.C. 1985, ch. C-46, art. 487.014.

25. Une demande *ex parte* s'entend d'une demande faite sans en aviser l'autre partie concernée.

26. Dans le cas d'un fournisseur de services qui se trouve dans un pays avec lequel le Canada a une entente d'entraide juridique, les organismes d'application de la loi peuvent actuellement avoir recours à la procédure d'entraide juridique. Selon cette procédure, la demande doit d'abord être soumise au ministère de la Justice du Canada avant d'être présentée à l'État étranger puis transmise au fournisseur de services étranger. Voir Ministère de la Justice Canada, *Modifications proposées aux lois sur l'accès aux renseignements en temps opportun (Projet de loi C-22 – Partie 1)*, document d'information; et Ministère de la Justice Canada, *Demandes d'entraide juridique présentées par le Canada*.

27. *Code criminel*, L.R.C. 1985, ch. C-46, art. 487.11. Au paragraphe 33 de l'arrêt *R. c. Paterson*, 2017 CSC 5, la Cour suprême du Canada estime que les « situations d'urgence » dénotent

> non pas simplement l'idée de commodité, d'avantage ou d'économie, mais plutôt d'urgence, une urgence découlant de circonstances qui commandent une intervention immédiate des policiers afin de préserver des éléments de preuve ou d'assurer la sécurité des policiers ou celle du public.

28. Ministère de la Justice Canada, *Modifications proposées aux lois sur l'accès aux renseignements en temps opportun (Projet de loi C-22 – Partie 1)*, document d'information.

29. *Loi sur l'entraide juridique en matière criminelle*, L.R.C. 1985, ch. 30 (4e suppl.).

30. *Ibid*., par. 2(1).

31. Le juge doit être convaincu qu'il existe des motifs raisonnables de soupçonner « qu'une infraction […] a été ou sera commise » et que les données « seront utiles à l'enquête relative à l'infraction ». *Code criminel*, L.R.C. 1985, ch. C-46, al. 487.016(2)a) et 487.016(2)b).

32. *Ibid*., art. 487.0198.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

33. *Loi réglementant certaines drogues et autres substances*, L.C. 1996, ch. 19.

34. *Loi sur le cannabis*, L.C. 2018, ch. 16.

35. L'article 487.011 du *Code criminel* définit les « données de transmission » comme des données techniques liées au fonctionnement d'une communication (composition, routage, adressage, signalisation) permettant d'indiquer certaines caractéristiques de celle-ci, sans en révéler la substance, le sens ou l'objet de la communication. Les métadonnées, quant à elles, n'ont pas de définition juridique. Selon le Commissariat à la protection de la vie privée du Canada, les métadonnées sont des données qui fournissent de l'information sur d'autres données et qui en décrivent le contexte d'utilisation. Ainsi, l'heure d'envoi et le numéro de destination d'un message texte sont des données de transmission, alors que le modèle de l'appareil ou l'identifiant technique du message constituent des métadonnées.

36. À l'étape de l'étude en comité, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a modifié l'alinéa 5(2)d) afin de réduire cette période d'un an à six mois.

37. À l'étape de l'étude en comité, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a modifié cette définition afin d'y intégrer un critère fondé sur des normes techniques internationales reconnues, de remplacer la notion de « risque sérieux » par celle de « risque crédible » et d'exclure certains risques liés à l'exercice de pouvoirs légaux d'accès à l'information découlant du régime de toute autre loi fédérale.

38. L'Office de surveillance des activités en matière de sécurité nationale et de renseignement est un organisme indépendant chargé d'examiner les activités du gouvernement du Canada en matière de sécurité nationale et de renseignement. Son mandat comprend notamment l'examen des activités exercées par les ministères et organismes fédéraux afin d'évaluer leur légalité, leur caractère raisonnable et leur nécessité, ainsi que de formuler des conclusions et des recommandations à cet égard (art. 8(1)a) à 8(1)c)).

39. L'article 1**3** de la Loi sur le soutien en matière d'accès autorisé à de l'information, tel que rédigée sous le projet de loi C-22, établit qu'un demandeur peut être l'une des personnes suivantes : le Ministre, tout employé du Service canadien du renseignement de sécurité, toute personne nommée ou employée sous le régime de la partie I de la *Loi sur la Gendarmerie royale du Canada* ou toute personne visée à l'art. 10 de cette loi, tout membre du personnel civil d'une autre force policière, ou tout agent de la paix au sens de l'art. 2 du *Code criminel*.

40. Sécurité publique Canada, *Loi sur le soutien en matière d'accès autorisé à de l'information (projet de loi C-22 – partie 2)*, document d'information.