CANADIAN CIVIL LIBERTIES ASSOCIATION | ASSOCIATION CANADIENNE DES LIBERTES CIVILES

MÉMOIRE PRÉSENTÉ AU COMITÉ SÉNATORIAL PERMANENT DE LA SÉCURITÉ NATIONALE, DE LA DÉFENSE ET DES ANCIENS COMBATTANTS AU SUJET DU PROJET DE LOI C-26, LOI CONCERNANT LA CYBERSÉCURITÉ, MODIFIANT LA LOI SUR LES TÉLÉCOMMUNICATIONS ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS

ASSOCIATION CANADIENNE DES LIBERTÉS CIVILES

Anaïs Bussières McNicoll | directrice du Programme des libertés fondamentales et directrice intérimaire du Programme de protection de la vie privée

Noa Mendelsohn Aviv | directrice générale et avocate générale

13 novembre 2024

Association canadienne des libertés civiles
124, rue Merton, bureau 400
Toronto (Ontario) M4S 2Z2
Téléphone : 416-363-0321
www.ccla.org/fr

Aperçu

L'Association canadienne des libertés civiles (ACLC) est une organisation nationale indépendante et non gouvernementale qui a été fondée en 1964 avec pour mandat de défendre et de promouvoir les libertés civiles, les droits de la personne et les droits démocratiques de toutes les personnes au Canada. Notre travail englobe la défense, la recherche et les litiges liés au système de justice pénale, aux droits à l'égalité, aux droits à la vie privée et aux libertés constitutionnelles fondamentales. Promouvoir la transparence et la responsabilité gouvernementale tout en garantissant une protection solide de la vie privée est au cœur de notre mandat.

La cybersécurité est une composante essentielle de la sécurité nationale, et l'écosystème numérique dans lequel nous vivons de plus en plus doit être sûr, fiable et à l'abri des menaces. La cybersécurité est également cruciale pour nos institutions démocratiques, l'économie, les infrastructures critiques, la défense nationale et la protection de notre vie privée en ligne. Il est donc important que le Canada prenne des mesures pour protéger les fondations numériques sur lesquelles repose la vie moderne.

Toutefois, la cybersécurité ne doit pas porter atteinte aux libertés civiles. Bien que le travail accompli par le Comité permanent de la sécurité publique et nationale de la Chambre des communes ait permis de répondre à certaines des préoccupations en matière de libertés civiles dans le cadre du projet de loi C-26, plusieurs questions doivent encore être abordées.

Le mémoire conjoint ci-joint sur le projet de loi C-26, que l'ACLC soutient, aborde les principales préoccupations non résolues dans quatre catégories de recommandations. Ces recommandations demandent que le projet de loi C-26 soit modifié pour 1) interdire au gouvernement de porter atteinte au chiffrement et à la sécurité des communications; 2) veiller à ce que les arrêtés du gouvernement ne puissent pas rester secrets indéfiniment; 3) remédier à d'importantes lacunes en matière de protection de la vie privée; 4) veiller à ce que tous les ministères et organismes gouvernementaux utilisent les renseignements obtenus en vertu du projet de loi C-26 exclusivement pour les activités de cybersécurité et d'assurance de l'information pour lesquelles les renseignements sont collectés.

Les mesures correctives recommandées répondent à des préoccupations pressantes susceptibles de saper la confiance du public tout en permettant à la législation d'atteindre ses objectifs déclarés : renforcer la cybersécurité dans les secteurs des services financiers, des télécommunications, de l'énergie et des transports, et aider les organisations à mieux se préparer aux incidents de cybersécurité, à y répondre et à les prévenir. Nous demandons instamment aux membres du comité d'adopter ces propositions visant à renforcer le projet de loi C-26.

Mémoire conjoint de la société civile présenté au Sénat pour son étude du projet de loi C-26

Association canadienne des libertés civiles
Canadian Constitution Foundation
Coalition pour la surveillance internationale des libertés civiles
Ligue des droits et libertés
Conseil national des musulmans canadiens
OpenMedia
Conseil du Canada de l'accès et la vie privée
M. Andrew Clement, professeur
M^me^ Brenda McPhail, Ph. D

Table des matières :

Résumé :..... 3

Recommandation 1 : Interdire au gouvernement de porter atteinte au chiffrement et à la sécurité des communications 5

Aperçu : *5*

Recommandation : *6*

Recommandation 2 : Veiller à ce que les arrêtés du gouvernement ne puissent pas rester secrets indéfiniment 8

Aperçu : *8*

Recommandation : *9*

Recommandation 3 : Corriger les graves lacunes du projet de loi C-26 en matière de protection de la vie privée 12

Aperçu : *12*

3.1 – Veiller à ce que l'autorisation judiciaire préalable soit requise, sauf dans des circonstances réellement urgentes, pour obtenir des renseignements confidentiels : *13*

3.2 – Résoudre l'incohérence entre la LPCSE et la Loi sur les télécommunications en ce qui concerne le traitement des renseignements personnels, y compris les renseignements dépersonnalisés : *15*

3.3 – Veiller à ce que des périodes de conservation des données soient attachées aux données des fournisseurs de télécommunications et aux divulgations de renseignements à l'étranger : *17*

Recommandation 4 : Limiter le CST à l'utilisation des renseignements obtenus en vertu du projet de loi C-26 exclusivement à des fins de cybersécurité et d'assurance de l'information. 19

Aperçu : *19*

Recommandation : *21*

Références et ressources : 23

Résumé :

Honorables Sénateurs et Sénatrices,

En tant qu'organisations et personnes engagées dans la défense des libertés civiles et du droit fondamental à la vie privée, nous partageons l'objectif du gouvernement du Canada de renforcer la cybersécurité dans les secteurs public et privé, et d'aider toute la population canadienne à mieux se protéger des cyberattaques.

Cependant, la forme actuelle du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois (« projet de loi C-26 » ci-après), contient des lacunes importantes qui peuvent compromettre les libertés civiles et la cybersécurité, et, par conséquent, la sécurité nationale.

La cybersécurité n'a aucune raison de porter atteinte aux libertés civiles. En effet, la confiance du public est essentielle pour que la cybersécurité soit menée à bien, surtout à une époque où la confiance du public dans les institutions démocratiques s'érode au Canada et dans le monde entier. Un projet de loi qui échoue au test de la légitimité démocratique ne renforcera pas la cybersécurité.

Nous avons d'abord exposé nos préoccupations dans une lettre conjointe présentée à l'honorable Marco Mendicino, ancien ministre de la Sécurité publique, en septembre 2022, et nous nous sommes réjouis que nos préoccupations aient été prises en compte par les députés de toutes les allégeances politiques à l'étape de la deuxième lecture du projet de loi C-26.

Nous avons ensuite soumis un ensemble détaillé de mesures correctives recommandées (français, English) aux membres du Comité permanent de la sécurité publique et nationale de la Chambre des communes (SECU). Plusieurs d'entre nous ont témoigné lors des audiences ultérieures en vue de fournir aux législateurs des renseignements supplémentaires.

Tout au long de ce travail, nous nous sommes inspirés des constations que l'expert Christopher Parsons a formulées dans son rapport intitulé *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* (EN ANGLAIS), qui a été publié par le Citizen Lab de l'Université de Toronto en octobre 2022.

Bien que le travail et le dévouement des membres du comité SECU et d'autres députés de tout l'horizon politique aient permis de résoudre certains problèmes de libertés civiles liés à la législation, plusieurs questions importantes et en suspens subsistent.

Compte tenu du fait qu'il reste plusieurs inquiétudes sérieuses en suspens, et du rôle constitutionnel du Sénat, nous croyons que vous avez un rôle essentiel à jouer pour veiller à ce que le projet de loi C-26 garantisse une cybersécurité solide, tout en protégeant la vie privée, en garantissant un sens des responsabilités et en faisant respecter les droits de toute la population canadienne.

Nous soulignons respectueusement les quatre domaines suivants comme étant des priorités à prendre en considération :

Projet de loi C-26 : recommandations prioritaires

1. **Interdire au gouvernement de porter atteinte au chiffrement et à la sécurité des communications**
2. **Veiller à ce que les arrêtés du gouvernement ne puissent pas rester secrets indéfiniment**
3. **Corriger les graves lacunes du projet de loi C-26 en matière de protection de la vie privée**
4. **Limiter le Centre de la sécurité des télécommunications Canada (CST) et les autres organismes gouvernementaux à utiliser les renseignements obtenus en vertu du projet de loi C-26 exclusivement à des fins de cybersécurité et d'assurance de l'information.**

Dans ce qui suit, nous fournissons plus de détails sur ces recommandations prioritaires. Nous sommes impatients de discuter de ces recommandations avec les membres du comité sénatorial lorsque vous commencerez à examiner le projet de loi C-26.

Recommandation 1 : Interdire au gouvernement de porter atteinte au chiffrement et à la sécurité des communications

Aperçu :

Le projet de loi C-26, tel qu'il a été adopté par la Chambre des communes, contient une dangereuse faille. Plus précisément, les nouveaux pouvoirs ministériels prévus au paragraphe 15.2(2) de la *Loi sur les télécommunications* pourraient être utilisés pour compromettre délibérément ou par inadvertance la sécurité et le chiffrement des réseaux de télécommunications dont dépendent, jour après jour, les citoyens et citoyennes, les gouvernements et les entreprises de partout au pays (et d'ailleurs).

C'est notamment le cas de l'alinéa 15.2(2)(l) qui donne au gouvernement le pouvoir d'exiger des fournisseurs de télécommunications qu'ils *« mettent en œuvre des normes qu'il précise relativement à leurs réseaux ou installations de télécommunications ou à leurs services de télécommunication »*.

Le danger réside dans le fait qu'un pouvoir aussi large soit utilisé pour contraindre les fournisseurs à adopter des normes qui *affaiblissent*, au lieu de *renforcer* le chiffrement et la protection de la vie privée. Dans sa formulation actuelle, la loi met en péril la liberté des citoyens canadiens de communiquer entre eux en privé, celle des entreprises de se lancer en toute sécurité dans le commerce national et international, ou celle des gouvernements et des représentants élus de bénéficier de communications privées.

Les experts en cybersécurité, au Canada et ailleurs, ont averti que la formulation actuelle de la loi mettait en danger l'économie du Canada, ses relations internationales et le droit fondamental à la vie privée de l'ensemble des Canadiens et Canadiennes :

- Kate Robertson et Ron Deibert, de Citizen Lab, ont écrit pour *The Globe & Mail* que les « *pouvoirs secrets, qui brisent le chiffrement* » [TRADUCTION] du projet de loi C-26 « *menacent la sécurité en ligne de tout le monde au Canada* » [TRADUCTION], et que le projet de loi « *habilite les représentants du gouvernement à ordonner secrètement aux entreprises de télécommunications d'installer des entrées interdites à l'intérieur des éléments chiffrés des réseaux du Canada* » [TRADUCTION].

- Dans son témoignage devant le comité parlementaire chargée d'étudier le projet de loi C-26, Eric Smith, vice-président principal de l'Association canadienne des télécommunications, a indiqué que le pouvoir de publier des décrets dans le cadre du projet de loi C-26 est *« très large »*, déclarant qu'il *« pourrait s'agir d'exiger, non pas nécessairement de retirer de l'équipement de votre infrastructure, mais d'en ajouter, ou de se conformer à certaines normes. Il pourrait s'agir d'un affaiblissement de l'encodage ou de l'obligation d'intercepter des communications »*.

- En citant les États-Unis comme un exemple d'excès du gouvernement que le Canada ne devrait pas imiter, l'Electronic Frontier Foundation a expliqué [EN ANGLAIS] que *« l'expérience des É.-U. offre un exemple à ne pas suivre et de ce qui peut arriver*

> *lorsqu'un gouvernement s'accorde de grands pouvoirs pour surveiller et diriger des réseaux de télécommunication, en l'absence de protections correspondantes pour les droits de la personne,* en prévenant que « *sans garanties adéquates, le projet de loi C-26 ouvrirait la porte à des pratiques et à des décrets similaires* » [TRADUCTION].

Bien qu'il ait reçu plusieurs mémoires (par exemple ici, ici, ici et ici) et entendu plusieurs témoins (par exemple ici, ici, ici et ici) sur ce sujet, le comité SECU n'a pas tenu compte de la question lors de son étude article par article du projet de loi C-26. La Chambre des communes n'a pas non plus eu l'occasion de le faire à l'étape du rapport, malgré le temps qui presse avant que les députés se penchent sur la question. Au lieu de cela, le projet de loi C-26 a été adopté à la hâte à l'étape du rapport, sans aucun débat.

Cette précipitation va à l'encontre des déclarations sans équivoque du gouvernement tout au long de l'examen du comité SECU, selon lesquelles l'objectif du projet de loi C-26 est la sécurité des réseaux, et non la surveillance.

Recommandation :

Le danger qui pèse sur la sécurité des communications des Canadiens et Canadiennes peut être résolu simplement, en précisant dans la loi quels types de normes entrent ou non dans son champ d'application :

Texte actuel de la *Loi sur les télécommunications*	**Correction recommandée à la *Loi sur les télécommunications* :**
Portée et teneur **15.2(2.1)** La portée et la teneur des dispositions du décret visé aux paragraphes (1) ou (2) sont raisonnables à la gravité des menaces d'ingérence, de manipulation, de perturbation ou de dégradation. **Précision** **15.2(2.2)** Il est entendu que, malgré le paragraphe (2), le ministre ne peut ordonner aux fournisseurs de services de télécommunication d'*intercepter*, au sens de l'article 183 du *Code criminel*, une *communication privée* ou une *communication radiotéléphonique*, au sens de cet article.	**Portée et teneur** **15.2(2.1)** La portée et la teneur des dispositions du décret visé aux paragraphes (1) ou (2) sont raisonnables à la gravité des menaces d'ingérence, de manipulation, de perturbation ou de dégradation. **Précision** **15.2(2.2)** Il est entendu que, malgré le paragraphe (2), le ministre ne peut ordonner aux fournisseurs de services de télécommunication d'*intercepter*, au sens de l'article 183 du *Code criminel*, une *communication privée* ou une *communication radiotéléphonique*, au sens de cet article. **Précision** **15.2(2.3)** Il est entendu que, malgré le paragraphe (2), le ministre n'est pas autorisé à prendre un arrêté qui compromettrait la confidentialité, la disponibilité ou l'intégrité d'une installation de télécommunications, d'un service de télécommunications ou d'une installation de transmission.

Cette recommandation vise à garantir que le gouvernement est habilité à prendre des arrêtés obligeant les fournisseurs de télécommunications à *renforcer* la confidentialité et la sécurité de leurs réseaux, mais pas à *les affaiblir*.

Cette modification vise à empêcher le gouvernement d'ordonner ou d'imposer aux fournisseurs de services de télécommunications qu'ils déploient ou activent (ou ont déployé ou activé) des capacités ou des pouvoirs portant sur l'accès légal au service de la « sécurisation » des infrastructures par le biais de l'adoption d'une norme. Si le gouvernement souhaite renforcer les pouvoirs d'ingérence légale, il doit le faire par l'entremise de processus législatifs distincts.

Partout au Canada, les particuliers et les entreprises s'appuient sur la solidité et la confidentialité des réseaux chiffrés pour assurer la sécurité de leurs communications. L'importance cruciale des communications sécuritaires est renforcée par le fait que le CST a récemment introduit le chiffrement de bout en bout sur le réseau canadien Très secret (RCTS) – voir la page 11 du récent rapport annuel du CST.

Qu'il s'agisse du CST, d'une grande entreprise, d'une petite entreprise, de représentants politiques ou de voisins qui échangent des nouvelles et des points de vue, tout le monde au Canada doit pouvoir avoir confiance dans la sécurité de ses communications. C'est précisément ce que garantira cette recommandation.

Recommandation 2 : Veiller à ce que les arrêtés du gouvernement ne puissent pas rester secrets indéfiniment

Aperçu :

Le libellé actuel du projet de loi C-26 permet au gouvernement de garder secret tout ordre donné aux fournisseurs de télécommunications et aux exploitants désignés en vertu de la *Loi sur la protection des cybersystèmes essentiels* (LPCSE). Selon le libellé actuel du projet de loi C-26, tel que modifié par la Chambre des communes, il est interdit aux fournisseurs de télécommunications et aux exploitants désignés de divulguer l'existence de l'arrêté ou de son contenu.

Nous comprenons que le secret puisse être garanti dans certaines circonstances; mais le secret devrait ni être la règle par défaut ni être autorisé à rester en place indéfiniment. Dans une démocratie, le gouvernement doit veiller à ce que les citoyens puissent comprendre comment il exerce ses pouvoirs en matière de cybersécurité et autres, à quelle fréquence et dans quel but, afin que les décideurs puissent être tenus de rendre des comptes.

La préoccupation abordée par cette recommandation est apparue au cours de l'examen du comité, lorsque la députée du Bloc québécois Kristina Michaud a proposé une modification, fondée étroitement sur notre mémoire au comité, qui aurait exigé une ordonnance de la Cour fédérale comme moyen de contrôle et d'équilibre contre les excès du gouvernement, afin de s'assurer que le gouvernement ne dissimule pas des mesures intrusives et disproportionnées sous le couvert du secret.

Les fonctionnaires du gouvernement se sont opposés à cette proposition de modification et ont fait valoir qu'elle *« pourrait entraîner des risques sur le plan de l'efficacité. Ainsi, un processus devant la Cour fédérale prendrait au moins quelques semaines »*. À l'appui de leur argumentation, ils ont cité de graves incidents de cybersécurité ayant nécessité une intervention urgente des pouvoirs publics et ont affirmé que la modification proposée pourrait entraver les interventions d'urgence.

La députée Jennifer O'Connell, secrétaire parlementaire du gouvernement pour la cybersécurité, a soutenu les préoccupations de la députée Michaud. Elle a proposé une autre modification exigeant un avis de tous les arrêtés, y compris les arrêtés confidentiels, au Comité des parlementaires sur la sécurité nationale et le renseignement et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). La modification du gouvernement a été adoptée et est maintenant intégrée à l'article 15.22 de la *Loi sur les télécommunications*, et au paragraphe 20(4) de la LPCSE.

Bien que la modification du gouvernement soit une étape importante et positive, **elle est loin de résoudre le problème principal : la possibilité pour les arrêtés de cybersécurité du gouvernement de rester secrets indéfiniment, sans que la validité de ce secret ne soit jamais examinée par un tribunal.**

Recommandation :

Nous reconnaissons qu'il y aura des occasions où le gouvernement devra prendre des mesures rapides en matière de cybersécurité et pourra déterminer que le délai nécessaire pour obtenir une ordonnance de la Cour fédérale est excessif dans les circonstances. En conséquence, **nous suggérons une modification révisée** pour reconnaître la nécessité d'une mesure extraordinaire dans des circonstances réellement urgentes, qui garantit également qu'un tribunal examinera la validité du secret de tous les arrêtés, dans un délai de 90 jours à compter de l'émission de chacun de ces arrêtés.

Cette recommandation imposerait une limite de 90 jours aux dispositions relatives à la confidentialité de tous les arrêtés, et toute prolongation nécessiterait que le gouvernement introduise une requête auprès de la Cour fédérale :

Texte actuel de la *Loi sur les télécommunications*	**Corrections recommandées à la *Loi sur les télécommunications* :**
Non-divulgation 15.1(2) Le décret peut aussi comprendre une disposition interdisant à toute personne de divulguer l'existence de celui-ci ou tout ou partie de son contenu.	**Non-divulgation** 15.1(2)a) Le décret peut aussi comprendre une disposition interdisant à toute personne de divulguer l'existence de celui-ci ou tout ou partie de son contenu, pour une période pouvant aller jusqu'à 90 jours après le jour où il est pris. 15.1 (2)b)(i) Le gouverneur en conseil peut saisir la Cour fédérale d'une demande d'ordonnance visant à prolonger la période pendant laquelle la divulgation de tout ou partie du contenu de l'arrêté pris en vertu du paragraphe (1) est interdite. La Cour fédérale peut rendre une ordonnance à cet effet lorsqu'elle est convaincue qu'il existe des motifs raisonnables de croire que la divulgation du contenu de l'arrêté, en totalité ou en partie, serait préjudiciable aux relations internationales, à la défense nationale ou à la sécurité nationale ou à la sécurité de toute personne. 15.1(2)b)(ii) Le juge, compte tenu des principes d'équité et de justice naturelle, nomme un avocat spécial figurant sur la liste des personnes visées au paragraphe 85(1) de la *Loi sur l'immigration et la protection des réfugiés* aux fins de contester la demande du gouverneur en conseil.

Non-divulgation 15.2(3) L'arrêté visé aux paragraphes (1) ou (2) peut aussi comprendre une disposition interdisant à toute personne de divulguer l'existence de celui-ci ou tout ou partie de son contenu.	**Non-divulgation** 15.2 (3)a) L'arrêté visé aux paragraphes (1) ou (2) peut aussi comprendre une disposition interdisant à toute personne de divulguer l'existence de celui-ci ou tout ou partie de son contenu, pour une période allant jusqu'à 90 jours après le jour où il est pris. 15.2 (3)b)i) Le ministre peut saisir la Cour fédérale d'une demande d'ordonnance visant à prolonger la période pendant laquelle la divulgation de tout ou partie du contenu de l'arrêté pris en vertu des paragraphes (1) ou (2) est interdite. La Cour fédérale peut rendre une ordonnance à cet effet lorsqu'elle est convaincue qu'il existe des motifs raisonnables de croire que la divulgation du contenu de l'arrêté, en totalité ou en partie, serait préjudiciable aux relations internationales, à la défense nationale ou à la sécurité nationale ou à la sécurité de toute personne. 15.2 (3)b)(ii) Le juge, compte tenu des principes d'équité et de justice naturelle, nomme un avocat spécial figurant sur la liste des personnes visées au paragraphe 85(1) de la *Loi sur l'immigration et la protection des réfugiés* aux fins de contester la demande du ministre.

Une situation semblable s'applique à la LPCSE, qui permet au gouvernement de garder secret tout arrêté applicable à des exploitants désignés. Ce pouvoir est d'autant plus problématique qu'il n'existe pas de mécanisme d'avis public automatique pour les nouveaux arrêtés. Encore une fois, s'il existe certainement des situations dans lesquelles le secret peut être approprié, le secret ne devrait pas être la règle par défaut dans une démocratie solide comme celle du Canada.

La proposition de modification suivante permettrait aux exploitants désignés de divulguer l'existence d'une directive, mais pas son contenu, sauf dans la mesure nécessaire pour s'y conformer :

LPCSE **Texte actuel**	**LPCSE** **Corrections recommandées :**
Interdiction de communication 24 Il est interdit à tout exploitant désigné visé par une directive de cybersécurité d'en communiquer l'existence ou le contenu ou de permettre qu'ils le soient, sauf en conformité avec l'article 25.	**Interdiction de communication** 24 Il est interdit à tout exploitant désigné visé par une directive de cybersécurité d'en communiquer~~-l'existence ou~~ le contenu ou de permettre qu'il~~s~~ le soi~~en~~t, sauf en conformité avec l'article 25.

Cas où la communication est permise 25(1) L'exploitant désigné visé par une directive de cybersécurité ne peut en communiquer l'existence et le contenu que dans la mesure nécessaire pour s'y conformer.	**Cas où la communication est permise** 25(1) L'exploitant désigné visé par une directive de cybersécurité ne peut en communiquer ~~l'existence et~~ le contenu que dans la mesure nécessaire pour s'y conformer.

Enfin, le Comité mixte permanent d'examen de la réglementation joue un rôle essentiel dans le processus démocratique du Canada. Le projet de loi C-26 devrait être modifié de manière à ce que le Comité mixte permanent d'examen de la réglementation puisse obtenir, évaluer et rendre un verdict, qui doit être rapidement rendu public, sur tout règlement promulgué en vertu des projets de réforme proposés de la *Loi sur les télécommunications* et de la *Loi canadienne sur la protection des systèmes cybernétiques*.

Le Comité devrait également être habilité à obtenir et à évaluer les règlements en vertu de la *Loi sur les télécommunications* et modifiés en vertu du paragraphe 18 de la *Loi sur les textes réglementaires*, et à rendre un verdict les concernant.

Les articles suivants du projet de loi C-26, qui exemptent la législation de la *Loi sur les instruments statutaires*, devraient être soit supprimés, soit modifiés pour préciser que la *Loi sur les textes réglementaires* s'applique :

- Paragraphe 15.3(3) des modifications de la *Loi sur les télécommunications*
- Paragraphes 22(1), 34(2), 36(3), 43(2), 45(3), 52(2), 54(3), 61(2), 63(3), 70(3), 73(4), 80(2) et 82(3) de la *LPCSE*

L'intégration des recommandations ci-dessus améliorera considérablement la transparence et, par conséquent, la confiance du public dans la manière dont le gouvernement utilise les nouveaux pouvoirs considérables qu'il s'octroie.

Recommandation 3 : Corriger les graves lacunes du projet de loi C-26 en matière de protection de la vie privée

Aperçu :

Depuis que le projet de loi C-26 a été dévoilé pour la première fois en juin 2022, la protection de la vie privée est restée l'une de nos principales préoccupations. Dans notre lettre conjointe de septembre 2022 adressée à l'honorable Marco Mendicino, alors ministre de la Sécurité publique, nous avons lancé un avertissement :

> *« Le projet de loi C-26 habilite le gouvernement à recueillir de vastes catégories de renseignements auprès des exploitants désignés, en tout temps et sous réserve de toutes conditions. Cela peut permettre au gouvernement d'obtenir des informations personnelles identifiables et anonymisées et de les distribuer ensuite à des organisations nationales, voire étrangères. »*

Nous reconnaissons que certains progrès ont été accomplis sur ce front au fur et à mesure que le projet de loi C-26 progressait à la Chambre des communes :

- Les fournisseurs de télécommunications, qui conservent de grandes quantités de renseignements confidentiels sur la population canadienne, peuvent désormais définir les renseignements personnels et dépersonnalisés comme étant « confidentiels », ce qui a pour effet d'imposer des protections beaucoup plus strictes pour leur traitement, leur stockage et leur sauvegarde.

- La *Loi sur la protection des renseignements personnels* s'applique désormais explicitement aux dispositions relatives à l'échange de renseignements contenus dans les modifications de la *Loi sur les télécommunications* et dans la *LPCSE*.

Cependant, la vie privée des Canadiens et Canadiennes continue d'être menacée par les dispositions du projet de loi C-26. Les problèmes les plus flagrants sont les suivants :

- Le gouvernement peut toujours divulguer des renseignements confidentiels, obtenus auprès des fournisseurs de télécommunications, à quiconque, sans avoir obtenu au préalable une ordonnance de la Cour fédérale. Le gouvernement a fait valoir que ce pouvoir était nécessaire pour éviter les retards dans les réponses aux situations d'urgence; toutefois, la modification que nous proposons (voir ci-dessous) atténue ces préoccupations.

- Le comité SECU a créé une incohérence législative en s'abstenant d'adopter une modification qui aurait explicitement défini les renseignements personnels et dépersonnalisés comme « confidentiels » pour la *LPCSE*, comme elle l'a fait pour la *Loi sur les télécommunications*.

- Le comité SECU avait cherché à protéger la vie privée des Canadiens et Canadiennes en limitant les périodes de conservation des données (réf. : modification proposée par Kristine Michaud). Toutefois, cette modification a été annulée sans débat à l'étape du rapport, ce qui a eu pour effet de permettre la conservation potentiellement indéfinie des renseignements personnels des Canadiens et Canadiennes.

Nous vous encourageons vivement à remédier systématiquement à ces lacunes fondamentales au cours de votre étude du projet de loi C-26 et à mettre en œuvre les recommandations suivantes :

3.1 – Veiller à ce que l'autorisation judiciaire préalable soit requise, sauf dans des circonstances réellement urgentes, pour obtenir des renseignements confidentiels :

Dans sa version actuelle, le projet de loi C-26 permet au ministre d'exiger la divulgation de renseignements confidentiels, y compris des renseignements personnels et dépersonnalisés, de la part des fournisseurs désignés. Ce pouvoir étendu doit être soumis à des contrôles et à des contrepoids afin d'empêcher le ministre de collecter et de divulguer ensuite des renseignements potentiellement préjudiciables sans avoir obtenu au préalable une ordonnance de la Cour fédérale. Dans le cas contraire, les entreprises et les particuliers de tout le Canada seront exposés au risque sérieux de voir leurs renseignements les plus sensibles divulgués de manière inappropriée.

La législation devrait être modifiée de sorte que, avant que le gouvernement puisse contraindre un fournisseur de télécommunications à divulguer des renseignements personnels ou dépersonnalisés, il doive d'abord obtenir une ordonnance judiciaire pertinente de la part de la Cour fédérale, stipulant que les renseignements recueillis aux termes de cette ordonnance doivent être utilisés aux fins de prendre, de modifier ou de révoquer un arrêté pris en vertu des articles 15.1 ou 15.2 ou un règlement en vertu de l'alinéa 15.8(1)a), ou de vérifier le respect ou d'empêcher le non-respect d'un tel arrêté ou d'un tel règlement.

Reconnaissant qu'il y aura des occasions où des renseignements devront être divulgués de manière urgente, nos recommandations comprennent un accommodement pour les circonstances réellement urgentes, y compris une disposition pour le contrôle rétroactif par la Cour fédérale.

Texte d'origine de la *Loi sur les télécommunications*	**Corrections recommandées à la *Loi sur les télécommunications* :**
15.5 (3)c) le ministre estime que la communication est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation.	15.5 (3)c) sur demande à la Cour fédérale, un juge est convaincu par une dénonciation sous serment qu'il y a des motifs raisonnables de croire ~~le ministre estime~~ que la communication est nécessaire pour sécuriser le système canadien de télécommunication~~, notamment~~ face aux menaces d'ingérence, de manipulation ou de perturbation. 15.5 (3)d) si les conditions prévues à l'alinéa c) pour l'obtention d'une ordonnance de la Cour fédérale sont réunies, mais qu'en raison de circonstances urgentes nécessitant un besoin imminent de sécuriser le système canadien de télécommunication face aux menaces d'interférence, de manipulation ou de perturbation, il serait impraticable d'obtenir une ordonnance de la Cour fédérale. Dans ce cas, le ministre doit, dans un délai de 30 jours, présenter une demande auprès de la Cour fédérale et fournir des renseignements sous serment justifiant la divulgation.

3.2 – Résoudre l'incohérence entre la LPCSE et la Loi sur les télécommunications en ce qui concerne le traitement des renseignements personnels, y compris les renseignements dépersonnalisés :

Comme indiqué ci-dessus, la *Loi sur les télécommunications* définit maintenant explicitement les renseignements personnels et dépersonnalisés comme étant « confidentiels » à l'alinéa 15.5(1)d). Il s'agit d'une amélioration essentielle par rapport à la version initiale.

Toutefois, le texte législatif devrait également préciser que les renseignements personnels *incluent* des renseignements dépersonnalisés, car la définition des « renseignements personnels » comporte d'importantes protections de la *Loi sur la protection des renseignements personnels*.

Texte actuel de la *Loi sur les télécommunications*	**Corrections recommandées à la *Loi sur les télécommunications* :**
15.5(1) La personne qui fournit des renseignements en application de l'article 15.4 peut désigner comme confidentiels :	**15.5(1)** La personne qui fournit des renseignements en application de l'article 15.4 peut désigner comme confidentiels :
a) les secrets industriels;	**a)** les secrets industriels;
b) les renseignements financiers, commerciaux, scientifiques ou techniques qui sont de nature confidentielle et qui sont traités comme tels de façon constante par elle;	**b)** les renseignements financiers, commerciaux, scientifiques ou techniques qui sont de nature confidentielle et qui sont traités comme tels de façon constante par elle;
c) les renseignements dont la communication risquerait vraisemblablement soit de causer à une autre personne ou à elle-même des pertes ou profits financiers appréciables ou de nuire à sa compétitivité, soit d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins;	**c)** les renseignements dont la communication risquerait vraisemblablement soit de causer à une autre personne ou à elle-même des pertes ou profits financiers appréciables ou de nuire à sa compétitivité, soit d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins;
d) les renseignements personnels et les renseignements dépersonnalisés.	**d)** les renseignements personnels, ~~et~~ y compris les renseignements dépersonnalisés.

Définitions **(1.1)** Les définitions suivantes s'appliquent à l'alinéa (1)d). ***dépersonnaliser*** Modifier des renseignements personnels afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement. (*de-identify*) ***renseignements personnels*** S'entend au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*. (*personal information*)	**Définitions** **(1.1)** Les définitions suivantes s'appliquent à l'alinéa (1)d). ***dépersonnaliser*** Modifier des renseignements personnels afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement. (*de-identify*) ***renseignements personnels*** S'entend au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*. (*personal information*) **(1.2)** Tout renseignement fourni en vertu de l'article 15.4 qui est un renseignement personnel, y compris tout renseignement dépersonnalisé, est réputé confidentiel.

En outre, pour éviter tout doute, la *LPCSE* doit être harmonisée avec la *Loi sur les télécommunications* révisée en définissant de manière proactive les renseignements personnels, y compris les renseignements dépersonnalisés, comme étant confidentiels :

LPCSE **Texte actuel**	**LPCSE** **Corrections recommandées :**
Définitions ***renseignements confidentiels*** S'entend des renseignements qui sont obtenus sous le régime de la présente loi relativement à un cybersystème essentiel et, selon le cas : a) qui portent sur la vulnérabilité des cybersystèmes essentiels de l'exploitant désigné ou sur les méthodes employées pour leur protection et qui sont traités comme étant confidentiels de façon constante par l'exploitant désigné; b) dont la divulgation risquerait vraisemblablement de causer des pertes ou profits financiers appréciables à un exploitant désigné ou de nuire à sa compétitivité; c) dont la divulgation risquerait vraisemblablement d'entraver des négociations, notamment contractuelles, menées par un exploitant désigné. (*confidential information*)	**Définitions** ***renseignements confidentiels*** S'entend des renseignements qui sont obtenus sous le régime de la présente loi relativement à un cybersystème essentiel et, selon le cas : a) qui portent sur la vulnérabilité des cybersystèmes essentiels de l'exploitant désigné ou sur les méthodes employées pour leur protection et qui sont traités comme étant confidentiels de façon constante par l'exploitant désigné; b) dont la divulgation risquerait vraisemblablement de causer des pertes ou profits financiers appréciables à un exploitant désigné ou de nuire à sa compétitivité; c) dont la divulgation risquerait vraisemblablement d'entraver des négociations, notamment contractuelles, menées par un exploitant désigné. (*confidential information*) d) renseignement qui est un renseignement personnel, y compris tout renseignement dépersonnalisé.

Enfin, les renseignements personnels, y compris les renseignements dépersonnalisés, devraient *toujours* être considérés comme confidentiels, au lieu que cette décision soit laissée à la discrétion de l'entité qui les fournit. Pour ce faire, il convient d'adopter la recommandation 10 du mémoire du Citizen Lab à ce comité :

Texte actuel de la *Loi sur les télécommunications*	**Corrections recommandées à la *Loi sur les télécommunications* :**
Exception **15.5(3)** La communication et l'autorisation visées au paragraphe (2) peuvent être faites dans les cas suivants : a) la communication est légalement autorisée ou exigée; b) la personne qui a désigné les renseignements comme confidentiels consent à leur communication; c) le ministre estime que la communication est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation.	**Exception** **15.5(3)** La communication et l'autorisation visées au paragraphe (2) peuvent être faites dans les cas suivants : a) la communication est légalement autorisée ou exigée; b) la personne qui a désigné les renseignements comme confidentiels consent à leur communication, ou dans le cas de renseignements personnels ou dépersonnalisés, la personne à laquelle les renseignements se rapportent consent à leur divulgation. c) le ministre estime que la communication est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation.

3.3 – Veiller à ce que des périodes de conservation des données soient attachées aux données des fournisseurs de télécommunications et aux divulgations de renseignements à l'étranger :

Le projet de loi C-26 doit être modifié pour préciser que les renseignements obtenus des fournisseurs de services de télécommunications ou des exploitants désignés par la *LPCSE* ne seront conservés que le temps nécessaire pour prendre, modifier ou révoquer un arrêté en vertu de l'article 15.1 ou 15.2 ou un règlement en vertu de l'alinéa 15.8(1)a) de la *Loi sur les télécommunications*, ou de l'article 20 de la *LPCSE*, ou pour vérifier le respect ou empêcher le non-respect d'un tel arrêté ou d'un tel règlement.

Une modification appliquant des périodes de conservation aux renseignements recueillis auprès des exploitants désignés en vertu de la *LPCSE* qui avait été initialement adoptée par le comité SECU lors de son étude article par article a ensuite été annulée, sans débat, à l'étape du rapport.

Cette annulation soulève la question suivante : si le gouvernement affirme qu'il a besoin de recueillir des renseignements dans le but précis de prendre des arrêtés, pourquoi s'oppose-t-il à ce que leur conservation soit limitée à la période pendant laquelle elles sont nécessaires à cette fin?

Nous demandons instamment à votre comité de veiller à ce que les périodes de conservation des données s'appliquent à la *Loi sur les télécommunications* et à la *LPCSE*, et que ces clauses s'appliquent également à toute divulgation de renseignements à des organisations, à des entités et à des gouvernements étrangers *:*

CORRECTION RECOMMANDÉE à la *Loi sur les télécommunications* :

1. À ajouter après le paragraphe 15.7(2) :

« **Périodes de conservation des données**
(3) Tout renseignement recueilli ou obtenu en vertu de la présente Loi ne sera conservé que le temps nécessaire pour prendre, modifier ou révoquer un décret pris en vertu de l'article 15.1, un arrêté pris en vertu de l'article 15.2 ou un règlement en vertu de l'alinéa 15.8(1)a), ou pour vérifier le respect ou empêcher le non-respect d'un tel arrêté ou d'un tel règlement.

(4) Les délais de conservation doivent être communiqués à la personne auprès de laquelle le ministre, ou la personne désignée par le ministre en vertu de l'article 15.4, a recueilli les renseignements.

(5) Toute entente, tout protocole d'entente ou accord écrit entre le gouvernement du Canada et le gouvernement d'un pays étranger, une organisation internationale d'États ou une organisation internationale créée par les gouvernements d'États, doit comporter des clauses relatives aux délais de conservation et à la suppression des données afin que celles-ci ne soient conservées que pendant la durée nécessaire aux fins visées au paragraphe (1). »

MESURE CORRECTIVE RECOMMANDÉE À LA LPCSE :

1. À ajouter après le paragraphe 26(3) :

« **Périodes de conservation des données**
(4) Tout renseignement collecté ou obtenu en vertu de la présente Loi ne sera conservé que le temps nécessaire pour prendre, modifier ou révoquer un arrêté en vertu de l'article 20, ou pour vérifier le respect ou empêcher le non-respect d'un tel arrêté ou d'un tel règlement.

(5) Les délais de conservation doivent être communiqués à la personne auprès de laquelle le gouverneur en conseil a recueilli les renseignements.

(6) Toute entente, tout protocole d'entente ou accord écrit entre le gouvernement du Canada et le gouvernement d'un pays étranger, une organisation internationale d'États ou une organisation internationale créée par les gouvernements d'États, doit comporter des clauses relatives aux délais de conservation et à la suppression des données afin que celles-ci ne soient conservées que pendant la durée nécessaire aux fins visées au paragraphe (1). »

Recommandation 4 : Limiter le CST à l'utilisation des renseignements obtenus en vertu du projet de loi C-26 exclusivement à des fins de cybersécurité et d'assurance de l'information.

Aperçu :

Dans sa forme actuelle, le projet de loi C-26 autoriserait le CST, soit l'organisme canadien de renseignement sur les transmissions et de cybersécurité, à obtenir et à analyser les données relatives à la sécurité des entreprises auxquelles les Canadiens et Canadiennes confient leurs renseignements personnels les plus sensibles, y compris les fournisseurs de télécommunications, les institutions financières sous réglementation fédérale, les fournisseurs d'énergie et toute autre entité désignée en vertu de la *Loi canadienne sur la sécurité des produits de consommation* (LCSPC).

Le projet de loi C-26 constitue une extension spectaculaire des pouvoirs du CST en matière de collecte de renseignements. Cette extension pose problème, car l'utilisation par le CST des renseignements qu'il recueille n'est actuellement pas limitée à l'aspect cybersécurité de son mandat, et toute utilisation serait largement soumise à un examen a posteriori plutôt qu'à un contrôle en temps réel.

Le gouvernement nous assure que les nouveaux pouvoirs du CST en matière de collecte de renseignements sont nécessaires à des fins de cybersécurité, mais il ne s'ensuit pas qu'il soit nécessaire ou proportionné d'utiliser ces pouvoirs élargis pour tous les aspects du mandat du CST. Comme le souligne un article récent [EN ANGLAIS] du professeur de droit Matt Malone, publié par le Centre pour l'innovation dans la gouvernance internationale, « *Ce changement diverge nettement de l'orientation de la loi habilitante du CST, qui cherche à imposer une plus grande responsabilité sur certains comportements au moyen d'autorisations et d'obligations d'examen.* » [TRADUCTION]

En bref, le projet de loi C-26 risque d'éroder les protections prudentes de la *Loi sur le Centre de la sécurité des télécommunications* qui empêchent le CST, dans certains aspects de son mandat, de diriger des actions contre des Canadiens ou des personnes au Canada, ou de recueillir des renseignements qui portent atteinte à l'attente raisonnable de protection de la vie privée d'une personne au Canada, atteinte contre laquelle nous protège notre *Charte*.

Il ne s'agit pas d'une simple menace théorique. Il ressort clairement du témoignage des fonctionnaires du CST, lors de l'étude article par article du comité SECU, que le CST a pleinement l'intention d'utiliser les renseignements qu'il recueille à des fins tant d'offense que de défense, et qu'il a également l'intention de transmettre les renseignements qu'il recueille à ses partenaires du Groupe des cinq.

Interrogé sur une modification du Bloc québécois qui aurait limité l'utilisation par le CST des renseignements qu'il recueille, Stephen Bolton (directeur général, Politique stratégique) a répondu :

> *« Les renseignements recueillis par le CST pour un volet de son mandat* ***peuvent être utilisés par celui-ci dans un autre volet****, pourvu que les conditions particulières énoncées dans la* Loi sur le CST *soient respectées. Les renseignements ayant trait aux programmes de sécurité permettront au CST et à son centre de cybersécurité de mieux comprendre les risques associés à la chaîne d'approvisionnement des exploitants désignés, ainsi que les intentions d'une entité étrangère par sa pénétration dans les secteurs respectifs.*
>
> *Si le CST n'est pas en mesure de remplir l'ensemble de son mandat, sa compréhension des intentions des acteurs étrangers par rapport à nos infrastructures essentielles et des mesures d'atténuation stratégiques appropriées s'en trouverait grandement diminuée.* ***Toute restriction réduirait également la collaboration du CST avec ses partenaires du Groupe des cinq.*** *»* *[SOULIGNEMENT AJOUTE]*

En d'autres termes, le CST affirme que les nouveaux pouvoirs de collecte de renseignements que lui confère le projet de loi C-26 sont non seulement nécessaires à des fins de cybersécurité, mais qu'il entend également les utiliser pour soutenir les relations internationales avec les agences de renseignement d'origine électromagnétique d'autres pays. Si nos alliances sont importantes, les renseignements personnels des Canadiens et Canadiennes ne doivent pas servir de monnaie d'échange pour maintenir ces relations.

Ces risques pour la vie privée et la responsabilité démocratique sont exacerbés par un manque de transparence depuis longtemps [EN ANGLAIS]. L'absence de collaboration du CST avec l'OSSNR dans le cadre de ses enquêtes ou l'absence de suivi de ses recommandations en témoignent.

Par exemple, le CST a précédemment rejeté les recommandations de l'OSSNR pour qu'il « *obtienne de plus amples conseils juridiques concernant ses échanges d'informations entre les volets touchant la cybersécurité et le renseignement étranger de son mandat, plus précisément pour ce qui a trait à leur conformité aux dispositions de la Loi sur la protection des renseignements personnels* », proclamant en 2021 qu'il avait déjà reçu un avis juridique sur la question de la part du ministère de la Justice.

Malgré le refus du CST en 2021, l'OSSNR a réitéré sa recommandation dans son examen le plus récent publié en janvier 2024, constatant que « *Les échanges internes d'informations entre les volets RE et cybersécurité du mandat du CST n'ont pas été suffisamment examinés quant à leur conformité aux dispositions de la Loi sur la protection des renseignements personnels*. ».

En bref, tel qu'il est actuellement rédigé, le projet de loi C-26 risque de perpétuer une situation dans laquelle le CST interprète ses mandats – maintenant surchargés de renseignements personnels d'un nombre encore plus important de Canadiens – d'une manière qui a été jugée non conforme à la *Loi sur la protection des renseignements personnels* par son examinateur.

Le Sénat a le rôle et l'obligation d'empêcher la mauvaise manipulation des renseignements souvent les plus confidentiels des Canadiens et Canadiennes, spécialement étant donné son manque de collaboration de longue date avec les agences chargés des examens [EN ANGLAIS].

Recommandation :

Le projet de loi C-26 doit être modifié pour garantir que tous les ministères et organismes gouvernementaux, y compris le CST, utilisent les renseignements obtenus en vertu du projet de loi C-26 exclusivement pour les activités de cybersécurité et d'assurance de l'information pour lesquelles les renseignements ont été recueillis.

Les renseignements ne devraient pas être utilisés à d'autres fins, notamment le renseignement d'origine électromagnétique ou étranger, de soutien interministériel non relatif à la cybersécurité ou d'opérations cybernétiques actives ou de défense. Ces restrictions devraient s'appliquer à toutes les agences, y compris, mais sans s'y limiter, celles qui relèvent de la compétence du ministre de la Sécurité publique et de la Protection civile.

Texte d'origine de la *Loi sur les télécommunications*	**Corrections recommandées à la *Loi sur les télécommunications* :**
1. À AJOUTER après le paragraphe 15.6(2) : « 15.6(3) Les renseignements échangés conformément à l'article 15.6 ne peuvent être utilisés par la personne qui les reçoit qu'à des fins exclusivement liées à la protection du système canadien de télécommunications contre les menaces d'ingérence, de manipulation ou de perturbation. »	

LPCSE Texte original	**LPCSE Corrections recommandées :**
Conseils du Centre de la sécurité des télécommunications 16 L'organisme réglementaire compétent peut fournir au Centre de la sécurité des télécommunications tous renseignements, y compris confidentiels, concernant le programme de cybersécurité d'un exploitant désigné ou toute mesure prise en application de l'article 15 afin que le Centre lui prodigue des avis, des conseils et des services conformément à son mandat concernant l'exercice des attributions qui lui sont conférées sous le régime de la présente loi.	**Conseils du Centre de la sécurité des télécommunications** 16 L'organisme réglementaire compétent peut fournir au Centre de la sécurité des télécommunications tous renseignements, y compris confidentiels, concernant le programme de cybersécurité d'un exploitant désigné ou toute mesure prise en application de l'article 15 afin que le Centre lui prodigue des avis, des conseils et des services conformément à son mandat de cybersécurité et d'assurance de l'information tel que décrit dans l'article 17 de la *Loi sur la Centre de la sécurité des télécommunications* concernant l'exercice des attributions qui lui sont conférées sous le régime de la présente loi.

2. À AJOUTER après le paragraphe 23(1) : « (2) Tout renseignement échangé conformément au paragraphe (1) ne peut être utilisée par la personne destinataire qu'aux fins prévues à l'article 5. »	
Renseignements confidentiels 26(3) Toute personne, toute agence ou tout organisme à qui sont communiqués des renseignements confidentiels en vertu du paragraphe (1) ou dont l'accès est autorisé en vertu de ce paragraphe les traite comme tels.	**Renseignements confidentiels** 26(3) Toute personne, toute agence ou tout organisme à qui sont communiqués des renseignements confidentiels en vertu du paragraphe (1) ou dont l'accès est autorisé en vertu de ce paragraphe les traite comme tels. **Restriction de l'utilisation :** 26(4) Les renseignements divulgués en vertu des paragraphes (1) ou (2) doivent être utilisés exclusivement à des fins liées à la protection des services critiques, des systèmes critiques ou des cybersystèmes essentiels.

Références et ressources :

Ressources principales :

- Texte intégral du projet de loi C-26 (tel qu'adopté en troisième lecture par la Chambre des communes)
- Résumé législatif C-26 (Bibliothèque du Parlement)
- Présentation conjointe au Comité permanent de la sécurité publique et nationale de la Chambre des Communes d'octobre 2023 (also in English).
- Témoignage devant le comité SECU des intervenants suivants : M. Andrew Clement, professeur, Mme Kate Robertson du Citizen Lab (partie 1, partie 2), M. Matt Hatfield d'OpenMedia, Mme Joanna Baron de la Canadian Constitution Foundation, Mme Sharon Polsky du Conseil du Canada de l'accès et la vie privée.
- Témoignage du Commissariat à la protection de la vie privée du Canada devant le comité SECU
- Lettre conjointe de la société civile de septembre 2022 (PDF) (aussi in English)
- Rapport de Chris Parsons du Citizen Lab : Cybersecurity will not thrive in darkness (PDF)

Couverture médiatique :

- Centre pour l'innovation dans la gouvernance internationale (éditorial de Matt Malone) : As Drafted, Canada's New Cybersecurity Law Opts for Secrecy over Security
- *The Globe and Mail*: Ottawa wants the power to create secret backdoors in our networks to allow for surveillance
- iPhoneinCanada: Feds Want Secret Backdoors for Network Surveillance: Experts
- National Observer/Centre pour l'innovation dans la gouvernance internationale (éditorial de Sharon Polsky) : The Road to Digital Hell is paved with Good Intentions
- The Hub: Trudeau promised radical transparency. Instead, he has exacerbated closed government (éditorial de Matt Malone)
- Balado de Michael Geist : Entrevue avec Kate Robertson du Citizen Lab sur le projet de loi C-26
- *Global News*: Contentious Liberal plan to overhaul cybersecurity faces more scrutiny
- *Presse canadienne* : Federal cybersecurity bill threatens privacy, transparency, civil society groups say (Jim Bronskill)
- News Forum - Canadian Justice: Bill C-26, Cybersecurity & Civil Liberties (L'animatrice Christine Van Geyn interviewe Dre Brenda McPhail [ACLC] et Rosa Addario d'OpenMedia)
- « Power Play », de CTV News : Entrevue avec Chris Parsons
- *Presse canadienne* : Liberal cybersecurity bill a "bad law" that must be amended, research report warns (Jim Bronskill)
- IT World Canada: Proposed telecom cybersecurity law gives Canadian government too much secret power: Researcher
- Options politiques : Don't give more powers to CSE until it submits to effective review (Dr Chris Parsons)
- *Hill Times*: Canadians' privacy could take a serious hit this coming legislative session (Ken Rubin)
- *Toronto Star* (éditorial d'OpenMedia): MPs must say no to agency request for powers to spy on your bank and travel records