Mémoire conjoint d'organisations de la société civile au Sénat sur le 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
Professeur Andrew Clement
Mme Brenda McPhail

Table des matières :

Mémoire conjoint d'organisations de la société civile au Sénat sur le projet de loi C-26 1

Sommaire : 2

Recommandation 1 : Interdire au gouvernement d'affaiblir le chiffrement et la sécurité des communications 4

Aperçu : 4

Recommandation : 5

Recommandation 2 : Veiller à ce que les décrets émanant du gouvernement ne restent pas secrets indéfiniment 7

Aperçu : 7

Recommandation : 8

Recommandation 3 : Corriger les graves lacunes du projet de loi C-26 en matière de protection de la vie privée 11

Aperçu : 11

3.1 - Veiller à exiger une approbation judiciaire préalable pour obtenir des renseignements confidentiels, sauf en situation d'urgence véritable : 12

3.2 - Résoudre l'incohérence entre la LPCE et la Loi sur les télécommunications en ce qui concerne le traitement des renseignements personnels, y compris les renseignements dépersonnalisés : 14

3.3 - Veiller à imposer des périodes de conservation aux données des fournisseurs de services de télécommunications et aux communications de renseignements à l'étranger : ..16

Recommandation 4 : Limiter exclusivement à des fins de cybersécurité et d'assurance de l'information l'utilisation des renseignements obtenus par le CST en

vertu du projet de loi C-26 18
Aperçu : *18*
Recommandation : *20*

Références et ressources : 22

Sommaire :

Honorables sénateurs et sénatrices,

En tant qu'organisations et particuliers déterminés à défendre les libertés civiles et le 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 tous les Canadiens à mieux se protéger contre les cyberattaques.

Cependant, la forme actuelle du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et d'autres lois en conséquence (ci-après le « projet de loi C-26 »), comporte des lacunes importantes qui pourraient compromettre les libertés civiles, la cybersécurité et, par conséquent, la sécurité nationale.

Il n'y a aucune raison de sacrifier les libertés civiles au profit de la cybersécurité. En effet, la confiance du public est essentielle au succès de la cybersécurité, surtout en cette période où la confiance envers les institutions démocratiques s'effrite au Canada et dans le monde entier. Un projet de loi qui ne respecte pas le critère de la légitimité démocratique ne pourra pas renforcer la cybersécurité.

Nous avons d'abord formulé nos préoccupations dans une lettre conjointe envoyée en septembre 2022 à l'ancien ministre de la Sécurité publique, Marco Mendicino, et nous avons été encouragés d'entendre les députés de tous les partis en faire état tout au long du débat en deuxième lecture du projet de loi C-26.

Nous avons ensuite présenté aux députés membres du Comité permanent de la sécurité publique et nationale (SECU) de la Chambre des communes un ensemble détaillé de mesures correctives recommandées (en anglais et en français). Lors des audiences suivantes, plusieurs d'entre nous ont témoigné afin d'apporter aux législateurs un complément d'information.

Tout au long de ces travaux, nous nous sommes inspirés des conclusions de l'expert Christopher Parsons, présentées dans son rapport d'octobre 2022 intitulé *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act*, 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 tous les horizons politiques aient permis de résoudre certains des problèmes de liberté civile posés par le projet de loi, il subsiste encore plusieurs questions importantes et non résolues.

Étant donné qu'il reste plusieurs sujets de vive préoccupation et compte tenu du rôle constitutionnel du Sénat, nous estimons qu'il vous incombe de veiller à ce que le projet de loi C-26 garantisse une cybersécurité stricte, tout en protégeant la vie privée et en assurant la reddition de comptes et le respect des droits de tous les Canadiens.

Nous vous soumettons respectueusement les quatre points suivants à titre de priorités :

Projet de loi C-26 : Recommandations prioritaires

1. **Interdire au gouvernement d'affaiblir le chiffrement et la sécurité des communications**
2. **Veiller à ce que les décrets émanant du gouvernement ne restent pas secrets indéfiniment**
3. **Corriger les graves lacunes du projet de loi C-26 en matière de protection de la vie privée**
4. **Limiter exclusivement à des fins de cybersécurité et d'assurance de l'information toute utilisation des renseignements obtenus par le CST et les autres organismes gouvernementaux en vertu du projet de loi C-26**

Nous donnons plus de détails sur ces recommandations prioritaires ci-dessous. Nous sommes impatients de discuter de ces recommandations avec les sénateurs lorsque vous commencerez à examiner le projet de loi C-26.

Recommandation 1 : Interdire au gouvernement d'affaiblir le chiffrement et la sécurité des communications

Aperçu :

Le projet de loi C-26, tel qu'adopté par la Chambre des communes, contient une lacune dangereuse. Plus précisément, les nouveaux pouvoirs ministériels énoncés au paragraphe 15.2(2) des modifications à la *Loi sur les télécommunications* pourraient servir à compromettre, délibérément ou par inadvertance, la sécurité des réseaux de télécommunications sur lesquels comptent tous les jours les citoyens, les gouvernements et les entreprises du Canada (et des autres pays).

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

Le danger, c'est qu'un tel pouvoir formulé de façon aussi large puisse être utilisé pour obliger les fournisseurs à adopter des normes qui *affaiblissent* le cryptage et la protection de la vie privée plutôt que de les *renforcer*. Dans sa forme actuelle, le libellé de la loi met en péril la liberté des gens au Canada de communiquer en privé les uns avec les autres, des entreprises de participer en toute sécurité au commerce national et international, ou des gouvernements et des représentants élus de disposer de communications privées.

Les experts en cybersécurité, au Canada et ailleurs, ont fait remarquer que le libellé actuel de la loi met en péril l'économie du Canada, ses relations internationales et le droit fondamental à la vie privée des gens partout au pays :

- Écrivant pour le *Globe & Mail*, Kate Robertson et Ron Deibert, de Citizen Lab, nous préviennent que les [TRADUCTION] *« pouvoirs secrets de décryptage »* prévus dans le projet de loi C-26 *« menacent la sécurité en ligne de tous les Canadiens »,* et que le projet de loi *« habilite les représentants du gouvernement à ordonner secrètement aux entreprises de télécommunications d'installer des "portes dérobées" à l'intérieur des éléments cryptés dans les réseaux du Canada. »*

- Dans son témoignage devant le comité parlementaire chargé d'étudier le projet de loi C-26, Eric Smith, premier vice-président de l'Association canadienne des télécommunications, a mentionné le pouvoir *« très large »* de publier des décrets que prévoit le projet de loi C-26, en déclarant que : *« 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. »*

- Citant les États-Unis comme un exemple d'intervention excessive du gouvernement que le Canada devrait éviter, l'Electronic Frontier Foundation a déclaré que [TRADUCTION] *« l'expérience des États-Unis offre une mise en garde sur ce qui peut arriver lorsqu'un*

gouvernement s'accorde de vastes pouvoirs pour surveiller et diriger les réseaux de télécommunications, en l'absence de protections correspondantes pour les droits de la personne ». Elle a aussi prévenu que *« en l'absence de garanties adéquates, le projet de loi C-26 pourrait ouvrir la porte à des pratiques et des décrets semblables ».*

Même s'il a reçu de multiples mémoires (p. ex. ici, ici, ici et ici) et entendu plusieurs témoins (p. ex. ici, ici, ici et ici) sur ce sujet, le SECU n'a pas examiné cette question lors de son étude article par article du projet de loi C-26. La Chambre des communes n'a pas non plus saisi l'occasion de le faire à l'étape du rapport, malgré les demandes pressantes adressées aux parlementaires. Au lieu de cela, le projet de loi C-26 a été adopté à toute vapeur à l'étape du rapport, sans débat.

Cette démarche va à l'encontre des déclarations sans équivoque du gouvernement tout au long de l'examen qu'a mené le SECU, à savoir que 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 peut être écarté pourvu qu'on indique clairement dans le texte les types de normes qui font partie ou non du champ d'application de la Loi :

Texte actuel de la Loi sur les télécommunications	**Modification 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*.	**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*. **Précision** **15.2 (2.3)** Il est entendu que, malgré le paragraphe (2), le ministre ne peut 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 conférer au gouvernement le pouvoir d'ordonner aux fournisseurs de services de télécommunications de *renforcer* la confidentialité et la sécurité de leurs réseaux, mais non de les *affaiblir*.

Cet amendement vise à empêcher le gouvernement d'ordonner ou d'exiger que les fournisseurs de services de télécommunication déploient ou activent (ou aient déployé ou activé) des capacités ou des pouvoirs liés à l'accès légal afin de « sécuriser » l'infrastructure par l'adoption d'une norme. Si le gouvernement souhaite renforcer ses pouvoirs d'interception légale, il doit le faire au moyen de processus législatifs distincts.

Partout au Canada, les particuliers et les entreprises comptent sur la solidité et la confidentialité des réseaux cryptés pour assurer la sécurité de leurs communications. L'importance cruciale des communications sécurisées est confirmée par le fait que le Centre de la sécurité des télécommunications (CST) a récemment introduit le cryptage 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 société, d'une petite entreprise, de représentants politiques ou de voisins qui échangent des nouvelles et des points de vue, il est essentiel pour tous les Canadiens de pouvoir avoir confiance dans la sécurité de leurs communications. C'est précisément ce que vise cette recommandation.

Recommandation 2 : Veiller à ce que les décrets émanant du gouvernement ne restent pas secrets indéfiniment

Aperçu :

Le libellé actuel du projet de loi C-26 permet au gouvernement de garder secret tout décret donné aux fournisseurs de services de télécommunications et aux exploitants désignés en vertu de la *Loi sur la protection des cybersystèmes essentiels* (*LPCE*). Selon le libellé actuel du projet de loi C-26, tel qu'amendé par la Chambre des communes, il est interdit aux fournisseurs de services de télécommunications et aux exploitants désignés de divulguer le fait qu'un décret a été émis, et encore moins son contenu.

Si nous comprenons qu'il peut être justifié dans certaines circonstances, le secret ne devrait pas être la norme par défaut ni être autorisé à demeurer en place indéfiniment. Dans une démocratie, le gouvernement doit veiller à ce que les citoyens puissent comprendre comment il exerce ses pouvoirs dans le domaine de la cybersécurité et dans les autres domaines, à quelle fréquence et dans quel but, afin que les décideurs puissent être dûment tenus de rendre compte.

La question sur laquelle porte cette recommandation a été soulevée lors de l'étude article par article du comité SECU, lorsque la députée du Bloc québécois, Kristina Michaud, a proposé un amendement – fondé en grande partie sur le mémoire que nous avons présenté au comité – qui aurait exigé une ordonnance de la Cour fédérale comme mesure de contrôle et d'équilibre contre les excès potentiels du gouvernement, afin que ce dernier ne puisse pas dissimuler des mesures d'intrusion disproportionnées sous le couvert du secret.

Les représentants du gouvernement se sont opposés à cette modification proposée et ont soutenu 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 argument, ils ont cité de graves incidents de cybersécurité ayant nécessité une intervention urgente du gouvernement, et ont affirmé que la modification proposée pourrait nuire aux interventions d'urgence.

La députée Jennifer O'Connell, secrétaire parlementaire du gouvernement pour la cybersécurité, a fait écho aux préoccupations de la députée Michaud. Elle a proposé un autre amendement exigeant un signalement de tous les décrets, y compris les décrets confidentiels, au Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). L'amendement du gouvernement a été adopté et figure désormais à l'article 15.22 de la *Loi sur les télécommunications* et au paragraphe 20(4) de la *LPCE*.

Bien que l'amendement du gouvernement soit une étape importante et positive, **il est loin de régler le problème fondamental, à savoir la possibilité que les décrets de cybersécurité du gouvernement demeurent secrets indéfiniment, sans que la validité de ce secret ne soit jamais examinée par un tribunal.**

Recommandation :

Nous reconnaissons que le gouvernement devra parfois prendre des mesures immédiates de cybersécurité, et qu'il pourra alors juger excessif le délai pour obtenir une ordonnance de la Cour fédérale dans ces circonstances. Par conséquent, **nous proposons un amendement révisé** pour reconnaître la nécessité de prendre des mesures extraordinaires dans des circonstances véritablement urgentes, mais garantissant aussi l'examen par un tribunal de la validité du secret de tous les décrets dans les 90 jours suivant leur émission.

Cette recommandation imposerait une limite de 90 jours aux dispositions de confidentialité de tous les décrets, et toute prolongation obligerait le gouvernement à présenter une demande à la Cour fédérale :

Texte actuel de la Loi sur les télécommunications	**Modifications 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 la date à laquelle il a été pris. 15.1 (2)b)(i) Le gouverneur en conseil peut demander à la Cour fédérale de proroger la période pendant laquelle la divulgation de tout ou partie du contenu du décret visé au paragraphe (1) est interdite. La Cour fédérale peut rendre une ordonnance à cet effet lorsqu'elle est convaincue qu'il y a des motifs raisonnables de croire que la divulgation de tout ou partie du décret porterait atteinte aux relations internationales, à la défense nationale ou à la sécurité nationale ou mettrait en danger la sécurité d'une personne. 15.1 (2)b)(ii) Le juge, en tenant compte des principes d'équité et de justice naturelle, nomme un conseiller spécial parmi les personnes visées au paragraphe 85(1) de la *Loi sur l'immigration et la protection des réfugiés* pour contester la demande du gouverneur en conseil.

Non-divulgation 15.2 (3) Le décret pris en vertu des 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) Le décret pris en vertu des 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 pouvant aller jusqu'à 90 jours après la date à laquelle il a été pris. 15.2 (3)b)(i) Le ministre peut demander à la Cour fédérale de proroger la période pendant laquelle la divulgation de tout ou partie du contenu du décret visé au paragraphe (1) ou (2) est interdite. La Cour fédérale peut rendre une ordonnance à cet effet lorsqu'elle est convaincue qu'il y a des motifs raisonnables de croire que la divulgation de tout ou partie du décret porterait atteinte aux relations internationales, à la défense nationale ou à la sécurité nationale ou mettrait en danger la sécurité d'une personne. 15.2 (3)b)(ii) Le juge, en tenant compte des principes d'équité et de justice naturelle, nomme un conseil spécial parmi les personnes visées au paragraphe 85(1) de la *Loi sur l'immigration et la protection des réfugiés* pour contester la demande du ministre.

Une situation similaire s'applique à la *Loi sur la protection des cybersystèmes essentiels* (LPCE), qui permet au gouvernement de garder secret tout décret donné à des exploitants désignés. Cette situation est d'autant plus problématique qu'il n'existe pas de mécanisme automatique de notification publique pour les nouveaux décrets. Encore une fois, si le secret est certainement justifié dans certains cas, il ne devrait pas être la règle par défaut dans une démocratie bien établie comme celle du Canada.

La proposition d'amendement suivante permettrait aux exploitants désignés de révéler l'existence d'une directive, mais non son contenu, sauf dans la mesure nécessaire pour se conformer à la directive :

LPCE **Texte actuel**	**LPCE** **Amendements recommandés**
Interdiction de divulgation 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 divulgation** 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 clé dans le processus démocratique du Canada. Le projet de loi C-26 devrait être amendé de manière à permettre au Comité mixte permanent d'examen de la réglementation d'obtenir le texte de tout règlement promulgué en vertu du projet de réforme de la *Loi sur les télécommunications* et de la *Loi sur la protection des cybersystèmes essentiels* du Canada, de l'évaluer et de prononcer un verdict qui doit être rendu public dans les plus brefs délais.

Le Comité devrait également être habilité à obtenir le texte de tout règlement adopté en vertu de la *Loi sur les télécommunications* et modifié conformément à l'article 18 de la *Loi sur les textes réglementaires*, à l'évaluer et à prononcer un verdict qui doit être rendu public dans les meilleurs délais.

Les articles suivants du projet de loi C-26, qui exemptent la loi de la *Loi sur les textes réglementaires*, devraient être supprimés ou modifiés de façon à faire ressortir clairement que la *Loi sur les textes réglementaires* s'applique :

- Les modifications du paragraphe 15.3 (3) de la *Loi sur les télécommunications*.
- Les 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 LPCE

L'intégration des recommandations qui précèdent améliorera grandement la transparence et, par conséquent, la confiance du public quant à l'utilisation que le gouvernement fait des nouveaux pouvoirs considérables qu'il est en train de se donner.

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 demeure l'une de nos principales préoccupations. Dans notre lettre conjointe de septembre 2022 au ministre de la Sécurité publique de l'époque, Marco Mendicino, nous avons fait la mise en garde suivante :

> *« 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 réalisés sur ce plan au fur et à mesure que le projet de loi C-26 progressait à la Chambre des communes, notamment :

- Les fournisseurs de services de télécommunications, qui conservent en grandes quantités les renseignements les plus sensibles des Canadiens, peuvent désormais définir les renseignements personnels et dépersonnalisés comme étant « confidentiels », ce qui a pour effet d'imposer des mesures de protection beaucoup plus rigoureuses pour leur traitement, leur stockage et leur protection.

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

Cependant, la vie privée des Canadiens reste menacée par les dispositions du projet de loi C-26. Voici quelques-uns des problèmes les plus flagrants :

- Le gouvernement peut toujours communiquer à n'importe qui des renseignements confidentiels obtenus auprès des fournisseurs de télécommunications, sans avoir d'abord obtenu une ordonnance de la Cour fédérale. Le gouvernement a fait valoir que ce pouvoir était nécessaire pour éviter tout retard dans les interventions d'urgence. Or, notre proposition d'amendement (exposée ci-dessous) remédie à cet inconvénient.

- Le comité SECU a créé une incohérence législative en omettant d'adopter un amendement qui aurait défini explicitement les renseignements personnels et dépersonnalisés comme étant « confidentiels » pour la LPCE, comme il l'a fait pour la *Loi sur les télécommunications*.

- Le comité SECU avait cherché à protéger la vie privée des Canadiens en limitant les périodes de conservation des données (réf. : amendement de Kristine Michaud). Pourtant, cet amendement a été rejeté sans débat à l'étape du rapport, ce qui a pour effet de permettre une conservation à durée indéterminée des renseignements personnels des Canadiens.

Nous vous encourageons fortement à corriger systématiquement ces lacunes fondamentales lors de votre étude du projet de loi C-26 et à mettre en œuvre les recommandations suivantes :

3.1 - Veiller à exiger une approbation judiciaire préalable pour obtenir des renseignements confidentiels, sauf en situation d'urgence véritable :

Dans sa forme actuelle, le projet de loi C-26 permet au ministre d'exiger la communication de renseignements confidentiels – y compris des renseignements personnels et dépersonnalisés – auprès de fournisseurs désignés. Ce pouvoir de portée générale doit être assujetti à un système de contrôles et vérifications pour empêcher le ministre de recueillir et de communiquer par la suite des renseignements susceptibles d'être préjudiciables sans obtenir au préalable une ordonnance de la Cour fédérale. Autrement, les entreprises et les particuliers de tout le Canada seront exposés au risque grave de voir leurs renseignements les plus sensibles divulgués de façon inappropriée.

La loi devrait être modifiée sur le point suivant : avant de pouvoir contraindre un fournisseur de télécommunications à communiquer des renseignements personnels ou dépersonnalisés, le gouvernement serait tenu d'obtenir une ordonnance judiciaire pertinente de la Cour fédérale. Cette ordonnance prescrirait que les renseignements ainsi recueillis seront utilisés exclusivement pour prendre, modifier ou révoquer un décret visé à l'article 15.1 ou 15.2 ou un règlement visé à l'alinéa 15.8(1)a), pour vérifier si le décret ou le règlement est respecté ou pour prévenir tout manquement à leur égard.

Étant donné qu'il sera parfois nécessaire de communiquer des renseignements en urgence, nos recommandations prévoient des mesures d'adaptation en cas de situation véritablement critique, combinées à la possibilité d'un contrôle rétroactif par la Cour fédérale.

Texte original de la Loi sur les télécommunications	**Modifications 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 présentée à la Cour fédérale, un juge est convaincu, sur la foi de renseignements fournis sous serment, qu'il existe des motifs raisonnables de croire que ~~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 obtenir une ordonnance de la Cour fédérale sont réunies, mais qu'en raison de l'urgence de la situation impliquant un besoin imminent de protéger le système canadien de télécommunications contre la menace d'interférence, de manipulation ou de perturbation, il serait impossible dans les faits d'obtenir une ordonnance de la Cour fédérale. Dans ces circonstances, le ministre doit, dans les 30 jours, présenter une demande à la Cour fédérale et fournir sous serment des renseignements justifiant la communication.

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

Comme il a été mentionné précédemment, la *Loi sur les télécommunications* définit maintenant explicitement à l'alinéa 15.5(1)d) les renseignements personnels et dépersonnalisés comme étant « confidentiels ». Il s'agit d'une amélioration très importante par rapport au projet initial.

Toutefois, le libellé de la loi devrait également préciser que les renseignements dépersonnalisés *sont inclus* dans les renseignements personnels, parce que la définition de « renseignements personnels » est assortie d'importantes protections dans la *Loi sur la protection des renseignements personnels*.

Texte actuel de la Loi sur les télécommunications	**Modifications 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	**(c)** les renseignements dont la communication risquerait vraisemblablement soit
(i) de causer à une autre personne ou à elle-même des pertes ou profits financiers appréciables	**(i)** de causer à une autre personne ou à elle-même des pertes ou profits financiers appréciables
(ii) ou de nuire à sa compétitivité, soit	**(ii)** ou de nuire à sa compétitivité, soit
(iii) d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins;	**(iii)** 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~~, ce qui inclut les renseignements dépersonnalisés.

Définitions **(1.1)** Les définitions qui suivent 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 qui suivent 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)** Les renseignements fournis en vertu de l'article 15.4 qui sont des renseignements personnels, ce qui inclut les renseignements dépersonnalisés, sont considérés comme confidentiels.

En outre, pour éviter toute ambiguïté, il faudrait adapter la LPCE à la *Loi sur les télécommunications* révisée en désignant de façon proactive les renseignements personnels comme étant confidentiels, et ce, en y incluant les renseignements dépersonnalisés :

LPCE **Texte actuel**	**LPCE** **Amendements recommandés**
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. (d) qui sont des renseignements personnels, ce qui inclut les renseignements dépersonnalisés. (*confidential information*)

Enfin, il faudrait *toujours* considérer comme confidentiels les renseignements personnels, y compris les renseignements dépersonnalisés, plutôt que de laisser cette décision à la discrétion de l'entité qui les fournit. Pour ce faire, il conviendrait d'adopter la recommandation 10 du rapport présenté par Citizen Lab au Comité :

Texte actuel de la Loi sur les télécommunications	**Modifications 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 étant 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 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.

3.3 - Veiller à imposer des périodes de conservation aux données des fournisseurs de services de télécommunications et aux communications de renseignements à l'étranger :

Il faut amender le projet de loi C-26 pour indiquer clairement que les renseignements obtenus auprès des fournisseurs de services de télécommunications ou des exploitants désignés par la LPCE ne seront conservés que pendant la période nécessaire pour prendre, modifier ou révoquer un décret pris en vertu des articles 15.1 ou 15.2 ou un règlement pris en vertu de l'alinéa 15.8(1)a) de la *Loi sur les télécommunications* ou de l'article 20 de la LPCE, pour vérifier la conformité au décret ou au règlement ou pour prévenir tout manquement à leur égard.

Un amendement qui imposait des périodes de conservation des données aux renseignements recueillis auprès des exploitants désignés dans le cadre de la LPCE, initialement adopté par le comité SECU lors de son examen article par article, a ensuite été annulé – sans débat – à l'étape du rapport.

Cette situation suscite la question suivante : si le gouvernement prétend avoir 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 ils sont nécessaires à cette fin?

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

MODIFICATION RECOMMANDÉE – Loi sur les télécommunications :

1. Ajouter après le par. 15.7(2) le paragraphe suivant :

« **Périodes de conservation des données**
(3) Les renseignements recueillis ou obtenus en vertu de la présente loi ne seront conservés que pendant la durée nécessaire à la prise, à la modification ou à la révocation d'un décret pris en vertu des articles 15.1 ou 15.2 ou d'un règlement pris en vertu de l'alinéa 15.8(1)a), à la vérification de la conformité avec le décret ou le règlement ou à la prévention de tout manquement à leur égard.

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

(5) Tout accord, entente ou arrangement conclu par écrit entre, d'une part, l'administration fédérale et, d'autre part, l'administration d'un État étranger, une organisation internationale d'États ou une organisation internationale établie par des gouvernements doit comporter des dispositions sur la conservation et la suppression des données afin que les renseignements ne soient conservés que le temps nécessaire aux fins prévues au paragraphe (1). »

MODIFICATION RECOMMANDÉE – LPCE :

1. Ajouter après le par. 26(3) le paragraphe suivant :

« **Périodes de conservation des données**
(4) Les renseignements recueillis ou obtenus en vertu de la présente loi ne seront conservés que pendant la période nécessaire à la prise, à la modification ou à la révocation d'un décret visé à l'article 20 ou à la vérification du respect ou à la prévention du non-respect de ce texte.

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

(6) Tout accord, entente ou arrangement conclu par écrit entre, d'une part, l'administration fédérale et, d'autre part, l'administration d'un État étranger, une organisation internationale d'États ou une organisation internationale établie par des gouvernements doit comporter des dispositions sur la conservation et la suppression des données afin que les renseignements ne soient conservés que le temps nécessaire aux fins prévues au paragraphe (1). »

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

Aperçu :

Dans sa forme actuelle, le projet de loi C-26 autoriserait le Centre de la sécurité des télécommunications (CST), l'organisme canadien du renseignement électromagnétique et de la cybersécurité, à obtenir et à analyser des données sur la sécurité provenant d'entreprises auxquelles les Canadiens confient leurs renseignements personnels les plus sensibles, notamment les fournisseurs de services de télécommunications, les institutions financières sous réglementation fédérale, les fournisseurs d'énergie et toutes les autres entités désignées dans la LPCE.

Le projet de loi C-26 représente un élargissement considérable des pouvoirs du CST en matière de collecte de renseignements. Cette expansion est problématique, car l'utilisation que fait actuellement le CST des renseignements qu'il recueille ne se limite pas à l'aspect cybersécurité de son mandat, et toute utilisation de sa part serait largement assujettie non pas à une surveillance en temps réel mais à un examen ultérieur.

Le gouvernement nous assure que les nouveaux pouvoirs du CST en matière de collecte de renseignements sont nécessaires pour la cybersécurité, mais il ne s'ensuit pas que le CST est obligé ou justifié d'utiliser ces pouvoirs élargis pour tous les aspects de son mandat. Comme le souligne un article récent du professeur de droit Matt Malone, publié par le Centre pour l'innovation dans la gouvernance internationale, [TRADUCTION] *« cela s'écarte nettement de l'objectif de la loi d'habilitation du CST, qui cherche à imposer une reddition de comptes accrue à l'égard de certaines conduites en exigeant des autorisations préalables et des examens »*.

En bref, le projet de loi C-26 risque d'éroder les protections soigneusement établies dans la *Loi sur le Centre de la sécurité des télécommunications* pour empêcher le CST, dans certains aspects de son mandat, de prendre des mesures à l'égard de Canadiens ou de personnes se trouvant au Canada, ou de recueillir des renseignements qui portent atteinte aux attentes raisonnables en matière de vie privée de toute personne au Canada, et qui sont protégées par notre *Charte*.

Il ne s'agit pas d'une menace théorique. Il ressort clairement du témoignage de ses représentants lors de l'examen article par article du SECU que le CST est bien résolu à utiliser les renseignements qu'il recueille à des fins tant offensives que défensives, et qu'il a également l'intention de les partager avec ses partenaires du Groupe des cinq.

Invité à commenter un amendement du Bloc qui aurait limité l'utilisation par le CST des renseignements qu'il recueille, Stephen Bolton (directeur général, Politique stratégique, CST) 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****. »* *[Caractères gras ajoutés]*

Autrement dit, le CST affirme non seulement que les nouveaux pouvoirs de collecte de renseignements que lui confère le projet de loi C-26 sont nécessaires à des fins de cybersécurité, mais qu'il entend également les utiliser pour entretenir ses relations internationales avec les agences de renseignement électromagnétique d'autres pays. Malgré l'importance de nos alliances, il ne saurait être question de se servir des renseignements personnels des Canadiens comme monnaie d'échange pour alimenter ces relations.

Ces risques pour la vie privée et pour la responsabilité démocratique sont exacerbés par le manque de respect pour la règle de transparence dont fait montre de longue date le CST. Ainsi, le CST a refusé de participer aux enquêtes de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et de donner suite à ses recommandations.

Par exemple, le CST a rejeté une recommandation de l'OSSNR visant à ce 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* », affirmant en 2021 qu'il avait déjà reçu des conseils juridiques du ministère de la Justice à ce sujet.

Malgré le refus du CST en 2021, l'OSSNR a réitéré sa recommandation dans son plus récent examen publié en janvier 2024, concluant que *« [l]es 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, dans son libellé actuel, le projet de loi C-26 risque de perpétuer une situation qui permet au CST d'interpréter ses mandats – maintenant enrichis des renseignements personnels d'un nombre encore plus grand de Canadiens – d'une manière que l'examinateur de ces mandats a jugée incompatible avec la *Loi sur la protection des renseignements personnels*. Le Sénat a le rôle et l'obligation d'empêcher une telle utilisation abusive des informations souvent les plus sensibles des Canadiens, d'autant plus que, depuis longtemps, le CST refuse de coopérer avec les organismes d'examen.

Recommandation :

Le projet de loi C-26 doit être modifié de manière à 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 ces renseignements sont recueillis.

Ces renseignements ne devraient pas être utilisés à d'autres fins, telles que les activités de renseignement électromagnétique ou étranger ou de soutien interministériel sans rapport avec la cybersécurité, ou les opérations cybernétiques actives ou défensives. Ces restrictions doivent s'appliquer à tous les organismes, y compris, mais sans s'y limiter, ceux qui relèvent du ministre de la Sécurité publique et de la Protection civile.

Texte original de la Loi sur les télécommunications	**Modifications recommandées à la Loi sur les télécommunications :**
1. AJOUTER après le par. 15.6(2) le paragraphe suivant : « 15.6(3) Les renseignements communiqués conformément à l'article 15.6 peuvent être utilisés par le destinataire exclusivement à des fins pertinentes à la protection du système canadien de télécommunications contre les menaces d'interférence, de manipulation ou de perturbation. »	

LPCE **Texte original**	**LPCE** **Amendements recommandés**
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 au mandat de cybersécurité et d'assurance de l'information du Centre de la sécurité des télécommunications énoncé à l'article 17 de la *Loi sur le CST*, concernant l'exercice des attributions qui lui sont conférées sous le régime de la présente loi.
2. Ajouter après le par. 23(1) le paragraphe suivant : « (2) Le destinataire des renseignements communiqués conformément au paragraphe (1) ne peut les utiliser 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. **Restrictions d'utilisation :** 26 (4) Les renseignements communiqués aux termes des paragraphes (1) ou (2) doivent être utilisés exclusivement à des fins de protection des services essentiels, des systèmes essentiels ou des cybersystèmes essentiels.

Références et ressources :

Principales ressources :

- Texte intégral du projet de loi C-26 (adopté en troisième lecture par la Chambre des communes)
- Projet de loi C-26 -- Résumé législatif (Bibliothèque du Parlement)
- Octobre 2023, présentation conjointe des organisations de la société civile au Comité permanent de la sécurité publique et nationale de la Chambre des communes (also in english)
- Témoignage au comité SECU par : professeur Andrew Clement, Kate Robertson / Citizen Lab (partie 1, partie 2), Matt Hatfield / OpenMedia, Joanna Baron / Canadian Constitution Foundation, Sharon Polsky / 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
- Sept. 2022 -- Lettre conjointe des organisations de la société civile (PDF) (also in english)
- Citizen Lab / rapport de Chris Parsons : Cybersecurity will not thrive in darkness (PDF)

Couverture médiatique :

- Centre pour l'innovation dans la gouvernance internationale (article d'opinion 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 (article d'opinion 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 (article d'opinion de Matt Malone)
- Balado de Michael Geist : Interview with Citizen Lab's Kate Robertson on Bill C-26
- Global News : Contentious Liberal plan to overhaul cybersecurity faces more scrutiny
- La 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 s'entretient avec Brenda McPhail (ACLC) et Rosa Addario d'OpenMedia)
- CTV News Power Play : Interview with Dr Chris Parsons
- La 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
- Policy Options : Don't give CSE more powers until it submits to effective review (Chris Parsons)
- Hill Times : Canadians' privacy could take a serious hit this coming legislative session (Ken Rubin)
- Toronto Star (lettre d'opinion par OpenMedia) : MPs must say no to agency request for powers to spy on your bank and travel records