

CANADIAN
CIVIL LIBERTIES
ASSOCIATION



ASSOCIATION
CANADIENNE DES
LIBERTES CIVILES

Mémoire présenté au Comité permanent de la sécurité publique
et nationale de la Chambre des communes 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

Daniel Konikoff | directeur par intérim, Vie privée, technologie et surveillance

Tashi Alford-Duguid | avocat-conseil à l'interne

Noa Mendelsohn Aviv | directrice générale et avocate générale

Le 12 septembre 2023

Association canadienne des libertés civiles

124, rue Merton, bureau 400

Toronto (Ontario) M4S 2Z2

Tél. : 416-363-0321

Table des matières

Introduction.....	2
Définir la notion de renseignements personnels.....	3
Traitement des renseignements personnels	4
Responsabilisation pour le traitement inapproprié des renseignements.....	8
Conclusion	9

Introduction

Fondée en 1964, l'Association canadienne des libertés civiles (ACLC) est un organisme non gouvernemental national indépendant qui a pour mandat de défendre et de promouvoir les libertés civiles, les droits de la personne et les libertés démocratiques de tous les Canadiens. Notre travail englobe la défense des droits, la recherche et les litiges liés au système de justice pénale, au droit à l'égalité, au droit à la vie privée et aux libertés constitutionnelles fondamentales. Le noyau central de notre mandat consiste à œuvrer pour favoriser la transparence et la reddition de comptes du gouvernement et pour garantir de solides mesures de protection de la vie privée.

Le présent mémoire de l'ACLC porte sur le projet de loi C-26, mesure législative proposée par le gouvernement du Canada en matière de télécommunications et de cybersécurité. Nous y traitons des préoccupations soulevées par le projet de loi en ce qui concerne les droits de la personne et les libertés civiles, en mettant particulièrement l'accent sur la protection de la vie privée. La cybersécurité est un élément essentiel de la sécurité nationale, et l'écosystème numérique de plus en plus présent dans nos vies doit être sécuritaire, fiable et à l'abri des menaces. La cybersécurité est également d'une importance cruciale pour nos institutions démocratiques, notre économie, nos infrastructures essentielles, la défense nationale et notre vie privée en ligne. Il est important que le Canada prenne des mesures pour protéger les fondements numériques sur lesquels reposent nos vies en ces temps modernes. Toutefois, dans sa forme actuelle, le projet de loi C-26 risque de compromettre notre droit à la vie privée, l'équité procédurale et les principes de gouvernance responsable, qui constituent le tissu même de notre démocratie. Le projet de loi C-26 ne doit pas être adopté sans que des révisions importantes y soient apportées afin de protéger les droits fondamentaux et l'équité procédurale.

Dans le présent mémoire, nous formulons des recommandations pour que le projet de loi C-26 améliore la façon dont le gouvernement et les entreprises de télécommunications définissent, traitent et protègent les renseignements personnels des particuliers et protègent ainsi leur droit à la vie privée. Après tout, la protection de la vie privée est une composante essentielle du sentiment de sécurité individuelle, tant en ligne qu'hors ligne, et doit occuper une place plus centrale dans le projet de loi C-26. L'ACLC estime que ses recommandations permettraient au projet de loi de mieux atteindre ses objectifs, à savoir renforcer la cybersécurité dans les secteurs des finances, des télécommunications, de l'énergie et des transports, et d'aider les organisations à mieux se préparer à prévenir les incidents de cybersécurité et à y répondre.

Les amendements décrits dans le présent mémoire font écho à la *Lettre de préoccupation conjointe* que l'ACLC et ses partenaires de la société civile ont publiée en septembre 2022¹. De plus, nos recommandations sont conformes à celles contenues dans la proposition d'amendements intitulée *Fixing Bill C-26 Recommended Remedies*,² dont l'ACLC est signataire, ainsi qu'aux recommandations du rapport de M. Christopher Parsons intitulé *Cybersecurity Will Not Thrive in Darkness*³.

Définir la notion de renseignements personnels

Dans sa forme actuelle, le projet de loi C-26 porte atteinte à la vie privée en permettant au gouvernement de recueillir de grandes catégories de renseignements auprès d'exploitants désignés, en tout temps et sous n'importe quelle condition, voire sans aucune condition. Le gouvernement serait ainsi en mesure d'obtenir des renseignements personnels nominatifs et dépersonnalisés et de les divulguer ensuite à des organisations nationales et peut-être étrangères. Compte tenu de la nature délicate des renseignements que la population canadienne fournit aux exploitants désignés, cette disposition pose un risque extraordinaire pour la vie privée des particuliers. Des mesures doivent être mises en place pour restreindre le pouvoir du gouvernement de collecter, d'utiliser et de communiquer les renseignements de nature délicate des particuliers.

En général, la confidentialité des renseignements personnels est l'une des clés d'une solide protection en matière de cybersécurité. Le fait d'intégrer la protection de la confidentialité dans la législation sur la cybersécurité contribuera grandement à assurer la réussite des mesures de protection en cybersécurité proposées dans le projet de loi C-26. Un certain degré de surveillance est nécessaire pour protéger l'infrastructure de télécommunications contre les attaques, mais cela ne doit pas se faire au détriment de la vie privée. Rien ne peut autoriser les gouvernements à surveiller et à analyser les activités en ligne sans que soient en place des mesures claires de protection de la vie privée et des droits fondamentaux des particuliers.

Pour restreindre raisonnablement la capacité du gouvernement à collecter des renseignements, on peut affiner la façon dont le projet de loi C-26 caractérise les renseignements qui méritent d'être protégés. Cela impliquerait de codifier les renseignements personnels et dépersonnalisés en tant que renseignements confidentiels. Les renseignements personnels sont tous les renseignements pouvant permettre d'identifier une personne par association ou déduction. De nombreux types de renseignements entrent dans la catégorie des renseignements personnels parce qu'ils peuvent permettre; selon le *Règlement général sur la protection des données* (RGPD) de l'Union européenne (UE), ces renseignements comprennent le nom d'une personne, ses numéros d'identification, ses données de localisation, ses identifiants en ligne ou les « éléments spécifiques

¹ McPhail, B. (28 septembre 2022), *Lettre de préoccupation conjointe concernant le projet de loi C-26*, ACLC, <https://ccla.org/fr/privacy/joint-letter-of-concern-regarding-bill-c-26/>

² Fix 26 Coordination Group (20 juin 2023), *Fixing Bill C-26: Recommended Remedies*. <https://drive.google.com/file/d/1pQn4-us3wf7qOIm2gI5scLQPGTaumkiO/view>

³ Parsons, C. (18 octobre 2022), *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act*, Citizen Lab, rapport de recherche n° 158.

propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale⁴ ».

De plus, les données personnelles peuvent être anonymisées ou dépersonnalisées, mais la dépersonnalisation des renseignements nécessite des protections supplémentaires. L'anonymisation consiste à supprimer de façon permanente les données d'identification, alors que la dépersonnalisation consiste à retirer divers fragments des renseignements d'identification et à les isoler les uns des autres ou à protéger les renseignements d'identification avec une méthode de chiffrement ou une clé (sans les supprimer définitivement). L'anonymisation des données est irréversible, tandis que les données dépersonnalisées peuvent être *repersonnalisées*. Les données dépersonnalisées nécessitent une meilleure protection que les données anonymisées; le projet de loi C-26 devrait donc veiller à ce que les renseignements dépersonnalisés soient explicitement reconnus comme confidentiels.

Dans leur état actuel, les modifications proposées à la *Loi sur les télécommunications* (LT) dans le projet de loi C-26 omettent de désigner les renseignements personnels et dépersonnalisés comme des renseignements confidentiels au sens du paragraphe 15.5(1). Il en va de même pour la *Loi sur la protection des cybersystèmes essentiels* (LPCE), où les renseignements personnels ou dépersonnalisés ne sont pas désignés confidentiels en vertu du paragraphe 6(1). Afin de protéger ces renseignements, les deux lois contenues dans le projet de loi C-26 doivent être modifiées pour mieux s'harmoniser avec nos droits à la protection de la vie privée, nos libertés et nos valeurs démocratiques.

AMENDEMENT RECOMMANDÉ - Loi sur les télécommunications :

1. Ajouter après l'alinéa 15.5(1)c) l'alinéa suivant :
d) « les renseignements personnels ou dépersonnalisés. »

Traitement des renseignements personnels

Le projet de loi C-26 accorde au ministre des pouvoirs excessifs pour le traitement des renseignements personnels. Les entreprises de télécommunications et les entreprises susceptibles d'être désignées en vertu de la LPCE recueillent, traitent et stockent de grandes quantités de données et de métadonnées personnelles, y compris les registres d'appels, les messages, les données financières et les données de localisation. Toutefois, dans sa forme actuelle, le projet de loi C-26 permet au ministre de communiquer ce type de renseignements personnels à toute personne désignée (*LT 15.6*) ou prévue par règlement (*LT 15.6* et *LPCE 23*). Que le gouvernement demande aux exploitants désignés des renseignements sur eux-mêmes et sur la façon dont ils se conforment aux ordonnances est une chose, mais une norme beaucoup plus stricte doit être en place lorsqu'il ordonne aux entreprises de lui fournir des renseignements sur leurs clients. Cela est particulièrement important pour les entreprises de télécommunications, étant donné le volume élevé de renseignements personnels qu'elles détiennent sur le public et la façon dont les données

⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) [2016] JO L 119/1.

de télécommunications peuvent être utilisées pour identifier les personnes, suivre leurs déplacements et surveiller leurs communications⁵. Le projet de loi C-26 devrait mieux protéger la confidentialité des communications et des renseignements personnels en créant une barrière plus efficace entre ces renseignements et la capacité du ministre de les divulguer. La loi devrait être modifiée de façon à exiger que le gouvernement obtienne une ordonnance judiciaire pertinente de la Cour fédérale avant de pouvoir obliger un fournisseur de services de télécommunications à divulguer des renseignements personnels ou des renseignements dépersonnalisés.

<i>Loi sur les télécommunications</i> Texte original	<i>Loi sur les télécommunications</i> Amendements recommandés
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.	<p>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 la communication est nécessaire pour sécuriser le système canadien de télécommunication notamment face aux menaces d'ingérence, de manipulation ou de perturbation.</p> <p>15.5 (3)d) le ministre estime qu'en raison de circonstances exceptionnelles démontrables, la communication est nécessaire pour sécuriser le système canadien de télécommunication face à une menace urgente d'ingérence, de manipulation ou de perturbation. Dans de telles circonstances, le ministre doit, dans les 30 jours, présenter une demande à la Cour fédérale et fournir sous serment des renseignements justifiant la communication.</p>

De plus, le Parlement devrait renforcer les mesures de protection de la vie privée prévues dans le projet de loi en ce qui concerne l'échange de renseignements avec des parties étrangères de la part des fournisseurs de services de télécommunications et des exploitants désignés. Le libellé du nouveau paragraphe 15.7(1) de la *Loi sur les télécommunications* se lit comme suit :

« Le ministre peut communiquer aux termes d'accords, d'ententes ou d'arrangements conclus par écrit entre, d'une part, l'administration fédérale et, d'autre part, l'administration d'une province ou d'un État étranger, une organisation internationale d'États ou une organisation internationale établie par des gouvernements, ou l'un de leurs organismes, des renseignements recueillis ou obtenus dans le cadre de la présente loi, à l'exception de renseignements désignés comme confidentiels en vertu du paragraphe 15.5(1), s'il croit qu'ils pourraient être utiles pour sécuriser le système canadien de

⁵ Parsons, C. (2015), *The Governance of Telecommunications Surveillance: How Opaque and Unaccountability Practices and Policies Threat Canadians*, disponible auprès du SSRN : <https://ssrn.com/abstract=2901521> ou <http://dx.doi.org/10.2139/ssrn.2901521>

télécommunications ou un système de télécommunications étranger, notamment face aux menaces d'ingérence, de manipulation ou de perturbation. »

De par sa portée et son imprécision, cette disposition non seulement paverait la voie à des interventions excessives de la part du ministre, mais elle pourrait aussi entraîner des risques d'atteinte à la vie privée au-delà des frontières provinciales et nationales et, de ce fait, des risques pour la vie et la sécurité des personnes et des groupes touchés. L'ACLC demande instamment que le projet de loi soit modifié de manière à empêcher le ministre de communiquer des renseignements personnels ou dépersonnalisés à des organisations ou des gouvernements étrangers, ainsi qu'à exiger que le ministre informe les fournisseurs de services de télécommunications et les exploitants désignés du moment où ces renseignements peuvent être divulgués et à qui ils peuvent l'être lorsque la partie destinataire est une organisation, une partie, un État ou un organisme étrangers.

AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :

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

« (2) Les personnes auprès desquelles le ministre a recueilli des renseignements en vertu de l'article 15.4, ou la personne qu'il a désignée à cette fin, sont informées du moment où ces renseignements ont été communiqués et de la partie destinataire à qui ils ont été communiqués lorsque celle-ci est un État étranger, une organisation internationale d'États ou une organisation internationale établie par le gouvernement d'un État. »

AMENDEMENT RECOMMANDÉ – LPCE :

3. Ajouter après le par. 27(1) le paragraphe suivant :

« (2) Les personnes, ou la personne qu'il désigne à cette fin, le ministre responsable ou l'organisme de réglementation, auprès desquels le ministre a recueilli des renseignements en vertu du paragraphe 26(1) sont informés du moment où ces renseignements ont été communiqués et de la partie destinataire à qui ils ont été communiqués lorsque celle-ci est un État étranger ou une organisation internationale établie par le gouvernement d'un État étranger. »

LPCE Texte original	LPCE Amendements recommandés
26 (1) Sous réserve du paragraphe (2), nul ne peut, sciemment, communiquer des renseignements confidentiels à une autre personne, à une agence ou à un organisme, ni en autoriser la communication ou l'accès, sauf dans les cas suivants :	26 (1) Sous réserve du paragraphe (2), nul ne peut, sciemment, communiquer des renseignements confidentiels, y compris des renseignements personnels ou dépersonnalisés, à une autre personne, à une agence ou à un organisme, ni en autoriser la communication ou l'accès, sauf dans les cas suivants :

Enfin, le projet de loi C-26 ne contient pas de dispositions rigoureuses concernant les périodes de conservation des données. Les données ne devraient être conservées que pendant la période où elles sont utiles, et le fait de stocker indéfiniment des données peut accroître les risques et les préjudices liés à d'éventuelles atteintes à la protection des données⁶. La période de conservation des données est cruciale pour veiller à ce que les renseignements obtenus en vertu de la *Loi sur les télécommunications* ou de la LPCE ne soient conservés que pendant la période où ils doivent servir à prendre une ordonnance législative ou à confirmer la conformité à une telle ordonnance. L'ACLC recommande que le projet de loi soit modifié pour restreindre autant que possible la période de conservation des données et pour y inclure — dans la mesure où la loi autorise le partage de données — l'obligation de joindre des clauses de conservation et de suppression des données aux ententes ou aux protocoles d'entente conclus avec des gouvernements ou des organismes étrangers.

AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :

4. Ajouter après le par. 15.7(2) les paragraphes suivants :

« Périodes de conservation des données

(3) 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 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) ou à la vérification du respect ou à la prévention du non-respect de l'un ou l'autre de ces textes.

(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 d'assurer que les renseignements ne sont conservés que le temps nécessaire aux fins prévues au paragraphe (1). »

AMENDEMENT RECOMMANDÉ – LPCE :

5. Ajouter après le par. 26(2) les paragraphes suivants :

« Périodes de conservation des données

(3) 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.

⁶ Commissariat à la protection de la vie privée du Canada, 2021, *Conservation et retrait des renseignements personnels : Principes et pratiques exemplaires*, CPVP. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/securite-des-renseignements-personnels/gd_rd_201406/

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

(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 d'assurer que les renseignements ne sont conservés que le temps nécessaire aux fins prévues au paragraphe (1). »

Responsabilisation pour le traitement inapproprié des renseignements

Le projet de loi C-26 ne prévoit aucune mesure de responsabilisation en matière de protection de la vie privée. La responsabilisation est un principe fondamental d'un gouvernement efficace et devrait également être un principe fondamental du projet de loi C-26.

L'une des principales préoccupations liées à la responsabilisation en matière de protection de la vie privée tient au fait que le projet de loi C-26 ne permet pas aux particuliers de demander réparation advenant que le gouvernement fasse un usage inapproprié de renseignements personnels ou dépersonnalisés. Le fait de permettre ce recours constituerait une mesure importante pour la responsabilisation en cas d'atteinte à la vie privée. L'ACLC recommande que le projet de loi C-26 soit modifié de manière à permettre aux particuliers de demander réparation si le gouvernement ou une partie à qui le gouvernement a divulgué leurs renseignements personnels ou dépersonnalisés perd par négligence le contrôle de ces renseignements et si cette perte de contrôle a une incidence sur la personne.

AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :

6. Ajouter après le par. 15.7(2) les paragraphes suivants :

Droit privé d'action

(3) Toute personne touchée par un acte ou une omission de la part du gouvernement, ou d'une personne ou une entité à laquelle le gouvernement a divulgué des renseignements confidentiels à son sujet, a un motif d'action en dommages-intérêts pour la perte ou le préjudice subi du fait de la violation dans les cas suivants :

- a. le gouvernement, ou la personne ou l'entité à qui le gouvernement a divulgué les renseignements confidentiels, perd le contrôle de ces renseignements;
- b. cette perte de contrôle cause des répercussions ou des préjudices importants pour la personne.

Délai de prescription

(4) Une action peut être intentée au plus tard deux ans à compter du jour où la personne prend connaissance de la perte de contrôle des renseignements confidentiels.

Tribunal compétent

(5) L'action visée au paragraphe (3) peut être intentée devant la Cour fédérale ou une cour supérieure d'une province.

AMENDEMENT RECOMMANDÉ – LPCE :

7. Ajouter après le par. 27(2) les paragraphes suivants :

Droit privé d'action

(3) Toute personne touchée par un acte ou une omission de la part du gouvernement, ou d'une personne ou une entité à laquelle le gouvernement a divulgué des renseignements confidentiels à son sujet, a un motif d'action en dommages-intérêts pour la perte ou le préjudice subi du fait de la violation dans les cas suivants :

- c. le gouvernement, ou la personne ou l'entité à qui le gouvernement a divulgué les renseignements confidentiels, perd le contrôle de ces renseignements;
- d. cette perte de contrôle cause des répercussions ou des préjudices importants pour la personne.

Délai de prescription

(4) Une action peut être intentée au plus tard deux ans à compter du jour où la personne prend connaissance de la perte de contrôle des renseignements confidentiels.

Tribunal compétent

(5) L'action visée au paragraphe (3) peut être intentée devant la Cour fédérale ou une cour supérieure d'une province.

Conclusion

Dans sa forme actuelle, le projet de loi C-26 porte atteinte à la vie privée et à l'équité procédurale. La protection de la vie privée et l'équité procédurale sont non seulement des éléments cruciaux de

la cybersécurité et de la protection de notre infrastructure essentielle, mais elles forment également le tissu même de notre démocratie. Le projet de loi donne au gouvernement le pouvoir de recueillir de grandes catégories de renseignements personnels sans protéger adéquatement les renseignements qui devraient être considérés comme confidentiels. Il menace également la vie privée et crée d'autres risques graves pour les personnes en permettant au gouvernement de divulguer des renseignements de nature sensible à des organisations nationales et étrangères sans mécanisme de contrôle approprié. De plus, le projet de loi contient des mécanismes inadéquats pour permettre aux personnes de demander réparation dans les cas où leurs renseignements personnels ont été traités de façon inappropriée et à mauvais escient.

Dans le présent mémoire, l'ACLC recommande des amendements qui répondent à ces préoccupations et qui permettent en même temps à la loi d'atteindre ses objectifs énoncés, soit renforcer la cybersécurité dans les secteurs des finances, des télécommunications, de l'énergie et des transports, et aider les organisations à mieux se préparer aux incidents de cybersécurité, à les prévenir et à y réagir. Nous exhortons les membres du Comité à adopter ces propositions visant à renforcer le projet de loi C-26.