

# Projet de loi C-26 : présentation conjointe au Comité permanent de la sécurité publique et nationale de la Chambre des Communes

*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  
Prof. Andrew Clement  
Brenda McPhail, Ph. D.*

## Sommaire

Mesdames, Messieurs,

En tant qu'organismes et personnes engagés dans la défense des libertés civiles, nous partageons l'objectif du gouvernement du Canada qui consiste à renforcer la cybersécurité et à aider les secteurs public et privé, ainsi que la population canadienne, à mieux se protéger contre les cyberattaques et autres cybermenaces.

Cependant, le projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois (ci-après le « projet de loi C-26 »), soulève plusieurs questions très préoccupantes relatives aux libertés civiles, à la protection de la vie privée et aux libertés démocratiques.

Dans une [lettre conjointe](#) déposée le 28 septembre 2022 à l'ancien ministre de la Sécurité publique, Marco Mendicino, nous avons expliqué en détail nos préoccupations concernant le projet de loi C-26 :

- risque de nouvelles obligations de surveillance;
- résiliation secrète de services essentiels;
- aucune protection pour limiter les abus;
- atteinte à la vie privée des personnes et des organismes;
- affaiblissement secret de la responsabilité et de la régularité de la procédure;
- prédominance des ordres inconnus sur la réglementation publique;
- présentation d'éléments de preuve secrets devant les tribunaux, ce qui est contraire aux principes de la justice fondamentale et des audiences publiques;
- pouvoirs sans surveillance ni responsabilité conférés au Centre de la sécurité des télécommunications (CST).

Nous nous réjouissons que nos préoccupations aient été exprimées par des députés de toutes les allégeances politiques tout au long du [débat](#) en deuxième lecture du projet de loi C-26.

Nous attirons l'attention des membres du Comité sur les mesures recommandées ci-jointes, qui répondent aux préoccupations relatives aux libertés civiles, et garantissent que le projet de loi C-26 offre une cybersécurité solide à tous les Canadiens tout en assurant la responsabilité et le respect de leurs droits.

Nos recommandations sont divisées en cinq grands axes :

1. [Limiter les pouvoirs ministériels](#)
2. [Protéger les renseignements personnels et professionnels confidentiels](#)
3. [Maximiser la transparence](#)
4. [Permettre aux avocats spéciaux de protéger l'intérêt public](#)
5. [Renforcer la responsabilité du CST](#)

Pour chacune de ces mesures, nous présentons un résumé de la situation et des recommandations.

Les amendements recommandés sont un mélange de recommandations législatives et narratives, et découlent principalement des constatations que Christopher Parsons (Ph. D.) 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](#) » (DISPONIBLE EN ANGLAIS UNIQUEMENT), publié par le Citizen Lab de l'Université de Toronto en octobre 2022, et auquel les députés ont fait référence à plusieurs reprises lors du débat en deuxième lecture.

Si la portée du rapport de M. Parsons est limitée aux modifications à la *Loi sur les télécommunications* présentes dans le projet de loi C-26, nous avons, le cas échéant, repris ses recommandations pour la *Loi sur la protection des cybersystèmes essentiels* (LPCE).

Nous estimons que nos recommandations répondent systématiquement aux préoccupations soulevées par les députés et qu'elles fournissent une base pour faire progresser rapidement cette loi dès la reprise des travaux du Parlement. Les recommandations permettent également au projet de loi C-26 d'atteindre ses [objectifs déclarés](#), soit de renforcer la cybersécurité dans les secteurs de la finance, des télécommunications, de l'énergie, du droit et des transports, d'interdire aux entreprises canadiennes d'utiliser des produits et des services provenant de fournisseurs à haut risque et d'aider les organismes et les particuliers à mieux se préparer et réagir aux cyberincidents et à les prévenir.

Nous sommes impatients de discuter de ces mesures recommandées avec les membres du Comité lors de l'examen du projet de loi C-26 cet automne.

Une copie en ligne de ce document est disponible à l'adresse suivante : <https://tinyurl.com/C26BriefSECU>

# Projet de loi C-26 : mesures recommandées

## Table des matières

<b>Mesure n° 1 : Limiter les pouvoirs ministériels</b>	<b>4</b>
Recommandation 1.1 – Les décrets et les arrêtés ministériels doivent être pertinents, proportionnés et raisonnables	4
Recommandation 1.2 – Les normes qui peuvent être imposées doivent être définies	6
<b>Mesure n° 2 : Protéger les renseignements personnels et professionnels confidentiels</b>	<b>8</b>
Recommandation 2.1 – Des mesures d’atténuation devraient être prévues si le gouvernement ne gère pas correctement les renseignements personnels ou dépersonnalisés	8
Recommandation 2.2 – Des périodes de conservation des données devraient être imposées aux données des fournisseurs de télécommunications et aux divulgations de renseignements à l’étranger	9
Recommandation 2.3 – Les fournisseurs de télécommunications et les exploitants désignés devraient être informés des parties étrangères qui reçoivent des renseignements à leur sujet	10
Recommandation 2.4 – La loi devrait délimiter les conditions dans lesquelles les renseignements d’un organisme privé peuvent être divulgués	10
Recommandation 2.5 – Définir les renseignements personnels comme des renseignements confidentiels, et interdire la divulgation de renseignements personnels ou dépersonnalisés à des organismes étrangers	11
Recommandation 2.6 – Autorisation judiciaire préalable pour l’obtention de renseignements personnels ou dépersonnalisés	12
<b>Mesure n° 3 : Maximiser la transparence</b>	<b>14</b>
Recommandation 3.1 – Remédier au manque de dispositions en matière de transparence et de responsabilité	14
Recommandation 3.2 – Les arrêtés devraient être publiés dans la Gazette du Canada	15
Recommandation 3.3 – Le ministre devrait être contraint de présenter des rapports concernant les arrêtés et les règlements	16
Recommandation 3.4 – Les consignes du silence devraient être limitées dans le temps	17
Recommandation 3.5 – Le CRTC devrait indiquer les arrêtés qui annulent des parties de ses décisions; un rapport annuel devrait indiquer le nombre de fois où des arrêtés et des règlements gouvernementaux prévalent sur les décisions du CRTC	18
Recommandation 3.6 – Tous les règlements devraient être accessibles au Comité mixte permanent d’examen de la réglementation	19
<b>Mesure n° 4 : Permettre aux avocats spéciaux de protéger l’intérêt public</b>	<b>22</b>
Recommandation 4.1 – Créer un poste d’avocat spécial pour permettre aux éléments de preuve d’être examinés dans un tribunal de droit sans être divulgués à des tiers	22
<b>Mesure n° 5 : Renforcer la responsabilité du Centre de la sécurité des télécommunications</b>	<b>27</b>
Recommandation 5.1 – Les renseignements obtenus ne devraient être utilisés que pour des activités de cybersécurité et d’assurance de l’information	27
<b>Références et ressources :</b>	<b>29</b>

## Mesure n° 1 : Limiter les pouvoirs ministériels

### Résumé du problème :

Plusieurs de nos préoccupations découlent des pouvoirs étendus que le projet de loi C-26 accorde au gouvernement à la suite des modifications apportées à l'article 15.2 de la *Loi sur les télécommunications* et à l'article 20 de la *Loi sur la protection des cybersystèmes essentiels*. Il s'agit des préoccupations suivantes :

- **Risque de nouvelles obligations de surveillance** : le projet de loi C-26 permet au gouvernement d'ordonner secrètement aux fournisseurs de télécommunications « [...] de faire quoi que ce soit ou s'abstenir de faire quoi que ce soit [...] ». Cela ouvre la porte à l'imposition d'obligations de surveillance aux entreprises privées et à d'autres risques tels que l'affaiblissement des normes de cryptage, ce que le public rejette depuis longtemps comme étant incompatible avec nos droits en matière de protection des renseignements personnels.
- **Risque de résiliation de services essentiels** : en vertu du projet de loi C-26, le gouvernement peut interdire à une personne ou à une entreprise de recevoir des services précis et interdire à toute entreprise d'offrir ces services à d'autres, par un arrêté gouvernemental secret. Cela ouvre la porte à des entreprises ou à des particuliers canadiens qui sont coupés des services essentiels sans explication. Le projet de loi C-26 n'établit aucun régime explicite, tel qu'un organisme de réglementation indépendant doté de pouvoirs solides, pour faire face aux effets collatéraux des arrêtés relatifs à la sécurité du gouvernement.
- **Aucune protection pour limiter les abus** : le projet de loi C-26 ne prévoit pas d'évaluation obligatoire de la proportionnalité, de la protection des renseignements personnels ou de l'équité, ni d'autres protections pour limiter les mauvais usages des nouveaux pouvoirs qu'il accorde au gouvernement (pouvoirs assortis d'amendes élevées, voire de peines d'emprisonnement, en cas de non-respect). Ces arrêtés s'appliquent à la fois aux entreprises de télécommunications et à un large éventail d'autres entreprises et organismes réglementés par le gouvernement fédéral et désignés en vertu de la *Loi sur la protection des cybersystèmes essentiels (LPCE)*. Des poursuites peuvent être engagées pour des violations présumées des arrêtés relatifs à la sécurité qui se sont produites jusqu'à trois ans auparavant.

### Amendements recommandés :

#### **Recommandation 1.1 – Les décrets et les arrêtés ministériels doivent être pertinents, proportionnés et raisonnables**

*(Cette recommandation est rédigée selon la recommandation 1 de M. Parsons)*

Les pouvoirs ministériels proposés dans le projet de loi C-26 vont bien au-delà des pouvoirs nécessaires pour sécuriser le secteur des télécommunications. Le projet de loi C-26 prévoit des pouvoirs que le ministre pourrait, entre autres, utiliser pour accéder aux renseignements personnels, ordonner aux exploitants de télécommunications d'espionner la population canadienne et priver les Canadiens de leur accès Internet.

L'ajout d'un critère de proportionnalité et de l'obligation de consulter des experts empêchera le ministre d'utiliser des problèmes sans importance pour justifier des actions disproportionnées ou intrusives. Le projet de loi devrait être amendé pour imposer des conditions supplémentaires concernant les circonstances particulières dans lesquelles le gouvernement peut exercer ses pouvoirs :

<b>Loi sur les télécommunications</b> <b>Texte original :</b>	<b>Loi sur les télécommunications</b> <b>Amendements recommandés :</b>
<p>15.2(1) S'il est d'avis que cela est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation, le ministre peut, par arrêté, après consultation du ministre de la Sécurité publique et de la Protection civile :</p> <p>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> <p>15.7(1) 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 télécommunications ou un système de télécommunications étranger, notamment face aux menaces d'ingérence, de manipulation ou de perturbation.</p>	<p>15.2(1) S'il est d'avis que cela est nécessaire pour sécuriser le système canadien de télécommunication, <del>notamment</del> face aux menaces d'ingérence, de manipulation ou de perturbation, le ministre peut, par arrêté, après consultation du ministre de la Sécurité publique et de la Protection civile :</p> <p>15.5(3)c) le ministre estime que la communication est nécessaire pour sécuriser le système canadien de télécommunication, <del>notamment</del> face aux menaces d'ingérence, de manipulation ou de perturbation.</p> <p>15.7(1) 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 télécommunications ou un système de télécommunications étranger, <del>notamment</del> face aux menaces d'ingérence, de manipulation ou de perturbation.</p>
<p>15.2(2) Le ministre peut, par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise – à l'exception d'une chose prévue au paragraphe 15.1(1) – et qu'il estime nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation. Il peut, entre autres, par le même arrêté :</p>	<p>15.2(2) Le ministre peut, par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise – à l'exception d'une chose prévue au paragraphe 15.1(1) – et qu'il estime nécessaire pour sécuriser le système canadien de télécommunication, <del>notamment</del> face aux menaces d'ingérence, de manipulation ou de perturbation. Il peut, <del>entre autres</del>, par le même arrêté :</p>
	<p>À ajouter après le paragraphe 15.2(2) :</p> <p>« (3) Aucun arrêté ne peut être pris en vertu des paragraphes (1) ou (2), à moins qu'il existe des motifs raisonnables de croire que l'arrêté est nécessaire, et que son champ d'application et son contenu sont proportionnés et raisonnables dans les circonstances.</p> <p>(4) Avant la prise d'un arrêté en vertu des paragraphes (1) ou (2), le ministre doit consulter</p>

	le ministre de la Sécurité publique et de la Protection civile et un groupe composé d'experts de l'industrie sur la nature et le contenu de l'arrêté. Le moment et la teneur de la consultation sont déterminés par le ministre, en tenant compte de la nature et de l'urgence des circonstances. »
--	---

LPCE Texte original :	LPCE Amendements recommandés :
20(1) Le gouverneur en conseil peut, par décret, donner des directives enjoignant à un exploitant désigné, individuellement ou au titre de son appartenance à une catégorie, de se conformer à toute mesure prévue dans la directive en vue de la protection d'un cybersystème essentiel.	« 20(1) Le gouverneur en conseil peut, par décret, donner des directives enjoignant à un exploitant désigné, individuellement ou au titre de son appartenance à une catégorie, de se conformer à toute mesure prévue dans la directive en vue de protéger un cybersystème essentiel contre une menace réelle. »
	À ajouter après le paragraphe 20(1) :  « (2) Aucun arrêté ne peut être pris en vertu du paragraphe (1), à moins qu'il existe des motifs raisonnables de croire que l'arrêté est nécessaire, et que son champ d'application et son contenu sont proportionnés et raisonnables dans les circonstances.  (3) Avant la prise d'un arrêté en vertu du paragraphe (1), le gouverneur en conseil doit consulter le ministre de la Sécurité publique et de la Protection civile et un groupe composé d'experts de l'industrie sur la nature et le contenu de l'arrêté. Le moment et la teneur de la consultation sont déterminés par le gouverneur en conseil, en tenant compte de la nature et de l'urgence des circonstances. »

## Recommandation 1.2 – Les normes qui peuvent être imposées doivent être définies

*(Cette recommandation est rédigée selon la recommandation 5 de M. Parsons)*

Le projet de loi devrait être amendé pour préciser clairement quels types de normes entrent ou non dans son champ d'application. Il convient de préciser qu'un arrêté ou un règlement imposant l'adoption de normes particulières ne peut être utilisé pour compromettre délibérément ou accidentellement la confidentialité, l'intégrité ou la disponibilité d'une installation de télécommunication, d'un service de télécommunication ou d'une installation de transmission.

<b>Loi sur les télécommunications</b> <b>Texte original</b>	<b>Loi sur les télécommunications</b> <b>Amendements recommandés :</b>
15.2(2)l) exiger qu'ils mettent en œuvre des normes qu'il précise relativement à leurs réseaux ou installations de télécommunication ou à leurs services de télécommunication.	15.2 (2)l) exiger qu'ils mettent en œuvre des normes qu'il précise relativement à leurs réseaux ou installations de télécommunication ou à leurs services de télécommunication. <b>Un arrêté ou un règlement imposant l'adoption de normes particulières ne doit pas être utilisé pour compromettre délibérément ou accidentellement la confidentialité, l'intégrité ou la disponibilité d'une installation de télécommunication, d'un service de télécommunication ou d'une installation de transmission.</b>

En outre, nous notons, en ce qui concerne particulièrement les députés, les recommandations suivantes de l'éminent Christopher Parsons (Ph. D.) :

- Recommandation 24 de M. Parsons : Tout le contenu de la loi doit être clair :** Le gouvernement devrait préciser comment les menaces prévues dans le cadre du projet de loi (« notamment face aux menaces d'ingérence, de manipulation ou de perturbation ») se comparent aux actes particuliers énoncés au paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications (Loi sur le CST)* (« tout méfait, toute utilisation non autorisée ou toute perturbation »), dans le but d'expliquer si les réformes de la *Loi sur les télécommunications* élargiraient, réduiraient ou aborderaient les mêmes catégories de lois que celles prises en compte dans la *Loi sur le CST*.
- Recommandation 25 de M. Parsons : Des définitions claires devraient être présentes dans la loi ou rendues publiques :** Le projet de loi devrait être amendé pour fournir des définitions claires des termes « ingérence », « manipulation » et « perturbation », ou pour faire référence à des définitions figurant dans d'autres lois particulières, ou encore pour ordonner au gouvernement de partager publiquement ces définitions et toute mise à jour ultérieure de ces définitions en dehors de la loi.

Enfin, nous notons que notre [recommandation 3.6](#), qui garantirait que tous les règlements pris en vertu du projet de loi C-26 soient accessibles au Comité mixte permanent d'examen de la réglementation, est également pertinente pour cette section. Cette recommandation est abordée dans la section « Maximiser la transparence » [ci-dessous](#).

## Mesure n° 2 : Protéger les renseignements personnels et professionnels confidentiels

### Résumé du problème :

Le projet de loi C-26 **porte atteinte à la vie privée** en autorisant le gouvernement à recueillir de vastes catégories de renseignements auprès d'exploitants désignés, à tout moment et sous n'importe quelles conditions, voire sans aucune condition. Le gouvernement pourrait ainsi obtenir des renseignements personnels identifiables et dépersonnalisés et les échanger ensuite à des organismes nationaux ou étrangers.

### Amendements recommandés :

#### **Recommandation 2.1 – Des mesures d'atténuation devraient être prévues si le gouvernement ne gère pas correctement les renseignements personnels ou dépersonnalisés**

*(Cette recommandation est rédigée selon la recommandation 14 de M. Parsons)*

Le projet de loi devrait être amendé pour permettre aux particuliers de demander réparation si le gouvernement ou une partie à laquelle le gouvernement a divulgué leurs renseignements personnels ou dépersonnalisés perd, par négligence ou involontairement, le contrôle de ces renseignements, et lorsque cette perte de contrôle a une incidence réelle sur la personne.

#### **AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :**

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

##### **Droit privé d'action**

(3) Toute personne touchée par un acte ou une omission du gouvernement, ou par une personne ou une entité à laquelle le gouvernement a divulgué des renseignements confidentiels, a un droit d'action en dommages-intérêts pour la perte ou le préjudice subi du fait de la contravention si :

- a) le gouvernement, ou la personne ou l'entité à qui le gouvernement a divulgué ses renseignements confidentiels, perd le contrôle de ces renseignements;
- b) cette perte de contrôle a une incidence réelle sur cette personne ou lui porte préjudice.

##### **Délai de l'action**

(4) L'action ne peut être intentée plus de deux ans après le jour où la personne a eu connaissance de la perte de contrôle de ses renseignements confidentiels.

##### **Juridiction compétente**

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

#### **AMENDEMENT RECOMMANDÉ – LPCE :**

1. À ajouter après le paragraphe 27(2) :

##### **Droit privé d'action**

(3) Toute personne touchée par un acte ou une omission du gouvernement, ou par une personne ou une entité à laquelle le gouvernement a divulgué des renseignements confidentiels, a un droit d'action en dommages-intérêts pour la perte ou le préjudice subi du fait de la contravention si :

- c) le gouvernement, ou la personne ou l'entité à qui le gouvernement a divulgué ses



- renseignements confidentiels, perd le contrôle de ces renseignements;  
d) cette perte de contrôle a une incidence réelle sur cette personne ou lui porte préjudice.

**Délai de l'action**

(4) L'action ne peut être intentée plus de deux ans après le jour où la personne a eu connaissance de la perte de contrôle de ses renseignements confidentiels.

**Juridiction compétente**

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

**Recommandation 2.2 – Des périodes de conservation des données devraient être imposées aux données des fournisseurs de télécommunications et aux divulgations de renseignements à l'étranger**

*(Cette recommandation est rédigée selon les recommandations 17 et 18 de M. Parsons)*

Le projet de loi doit être amendé afin de préciser que les renseignements obtenus auprès des fournisseurs de télécommunications ou des exploitants désignés par la LPCE ne seront conservés 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) de la *Loi sur les télécommunications* ou de l'article 20 de la LPCE, ou pour vérifier le respect ou empêcher le non-respect d'un tel arrêté ou d'un tel règlement. Les périodes de conservation doivent être communiquées aux fournisseurs de télécommunications auprès desquels le ministre a recueilli des renseignements.

Le projet de loi devrait également être amendé pour ordonner au gouvernement d'ajouter des clauses relatives aux délais de conservation et à la suppression des données dans les ententes ou les protocoles d'entente conclus avec des gouvernements ou des organismes étrangers.

**AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :**

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

**« Délais 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). »

**AMENDEMENT RECOMMANDÉ – LPCE :**

1. À ajouter après le paragraphe 26(2) :

**« Délais de conservation des données**

(3) 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.

(4) Les délais de conservation doivent être communiqués à la personne auprès de laquelle le gouverneur en conseil 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). »

### **Recommandation 2.3 – Les fournisseurs de télécommunications et les exploitants désignés devraient être informés des parties étrangères qui reçoivent des renseignements à leur sujet**

*(Cette recommandation est rédigée selon la recommandation 19 de M. Parsons)*

Le projet de loi devrait être amendé de manière à ce que les fournisseurs de télécommunications ou les exploitants désignés en vertu de la LPCE soient explicitement informés du moment et, le cas échéant, de la personne à laquelle les renseignements peuvent être divulgués lorsque le destinataire est un pays, une agence, un organisme ou une partie étrangère ou étranger :

#### **AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :**

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

« (2) Les personnes auprès desquelles le ministre, ou une personne désignée par le ministre, a recueilli des renseignements en vertu de l'article 15.4 sont informées du moment où ces renseignements ont été divulgués et de leur destinataire lorsque celui-ci est un pays étranger, une organisation internationale d'États ou une organisation internationale créée par les gouvernements d'États. »

#### **AMENDEMENT RECOMMANDÉ – LPCE :**

1. À ajouter après le paragraphe 27(1) :

« (2) Les personnes auprès desquelles le ministre, ou une personne désignée par le ministre, un ministre compétent ou un organisme réglementaire a recueilli des renseignements en vertu du paragraphe 26(1) sont informées du moment où ces renseignements ont été divulgués et de leur destinataire lorsque celui-ci est un pays étranger ou une organisation internationale créée par les gouvernements d'États étrangers. »

### **Recommandation 2.4 – La loi devrait délimiter les conditions dans lesquelles les renseignements d'un organisme privé peuvent être divulgués**

*(Cette recommandation est rédigée selon la recommandation 20 de M. Parsons)*

Le Parlement devrait restreindre les conditions sous lesquelles le ministre peut divulguer les renseignements d'un organisme privé :

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
15.7(1) 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 télécommunications ou un système de télécommunications étranger, notamment face aux menaces d'ingérence, de manipulation ou de perturbation.	15.7(1) Le ministre <del>peut</del> <b>ne doit</b> communiquer qu'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 <del>pourraient</del> <b>sont ou seront</b> utiles pour sécuriser le système canadien de télécommunications ou un système de télécommunications étranger, <del>notamment</del> face aux menaces d'ingérence, de manipulation ou de perturbation.

<b>LPCE Texte original</b>	<b>LPCE Amendements recommandés :</b>
27(2)b) le ministre, le ministre compétent ou l'organisme réglementaire, selon le cas, est convaincu qu'ils seront traités comme tels et ne seront pas autrement communiqués sans leur consentement exprès.	27(2)b) le ministre, le ministre compétent ou l'organisme réglementaire, selon le cas, est convaincu qu'ils seront traités comme tels et ne seront pas autrement communiqués sans leur consentement exprès, et  <b>c) le ministre, le ministre compétent ou l'organisme réglementaire estime que les renseignements sont ou seront utiles pour la protection des cybersystèmes essentiels. »</b>

### **Recommandation 2.5 – Définir les renseignements personnels comme des renseignements confidentiels et interdire la divulgation de renseignements personnels ou dépersonnalisés à des organismes étrangers**

*(Cette recommandation est rédigée selon la recommandation 28 et 30 de M. Parsons)*

Le projet de loi devrait être amendé afin de préciser que tous les renseignements personnels et dépersonnalisés divulgués par les fournisseurs de télécommunications, ou les fournisseurs désignés en vertu de la LPCE, sont classés comme des renseignements confidentiels et ne peuvent pas être divulgués à des gouvernements ou à des organismes étrangers.

**AMENDEMENT RECOMMANDÉ – Loi sur les télécommunications :**

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

<b>LPCE Texte original</b>	<b>LPCE Amendements recommandés :</b>
26(1) Sous réserve du paragraphe 26(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 26(2), nul ne peut, sciemment, communiquer des renseignements confidentiels, notamment 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 :

**Recommandation 2.6 – Autorisation judiciaire préalable pour l’obtention de renseignements personnels ou dépersonnalisés**

*(Cette recommandation est rédigée selon la recommandation 29 de M. Parsons)*

Le projet de loi, tel qu’il est formulé, permettrait au ministre de divulguer des renseignements personnels à n’importe qui. Il s’agit d’une erreur qui devrait faire l’objet d’un contrôle afin d’assurer que le ministre ne divulgue pas de renseignements préjudiciables sans avoir au préalable demandé une ordonnance à la Cour fédérale.

Le projet de loi devrait être amendé de telle sorte qu’avant que le gouvernement puisse contraindre un fournisseur de télécommunications à divulguer des renseignements personnels ou dépersonnalisés, il doit d’abord obtenir une ordonnance judiciaire pertinente de la Cour fédérale, lorsque les renseignements doivent être utilisés exclusivement 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 à un tel arrêté ou à un tel règlement.

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
--	---

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 information sous serment qu'il y a des motifs raisonnables de croire que ~~le ministre estime que~~ la communication est nécessaire pour protéger le système canadien de télécommunications, ~~notamment~~ contre les menaces d'ingérence, de manipulation ou de perturbation.

15.5(3)d) le ministre estime l'existence d'une situation d'urgence démontrable qui rend la communication nécessaire pour protéger le système canadien de télécommunications contre les menaces d'ingérence, de manipulation ou de perturbation. Sous l'existence d'une telle situation d'urgence, 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 communication.

En outre, nous prenons note des amendements recommandés pour imposer un devoir de confidentialité aux organismes réglementaires relatif aux documents qu'ils obtiennent en vertu des pouvoirs prévus aux articles 32, 41, 50, 59, 68 et 78 de la LPCE :

**AMENDEMENT RECOMMANDÉ – LPCE :**

1. À ajouter après le paragraphe 32(3) :  
« **Confidentialité**  
(4) Le surintendant assure la confidentialité de tout document, dossier ou système informatique retiré en vertu de l’alinéa 32(2)f) et de toute copie faite en vertu de l’alinéa 32(2)f). »
2. À ajouter après le paragraphe 41(3) :  
« **Confidentialité**  
(4) L’inspecteur assure la confidentialité de tout document, dossier ou système informatique retiré en vertu de l’alinéa 41(2)f) et de toute copie faite en vertu de l’alinéa 41(2)f). »
3. À ajouter après le paragraphe 50(3) :  
« **Confidentialité**  
(4) La personne désignée en vertu du paragraphe 49(1) assure la confidentialité de tout document, dossier ou système informatique retiré en vertu de l’alinéa 50(2)f) et de toute copie faite en vertu de l’alinéa 50(2)f). »
4. À ajouter après le paragraphe 59(3) :  
« **Confidentialité**  
(4) La personne désignée en vertu du paragraphe 58(1) assure la confidentialité de tout document, dossier ou système informatique retiré en vertu de l’alinéa 59(2)f) et de toute copie faite en vertu de l’alinéa 59(2)f). »
5. À ajouter après le paragraphe 68(3) :  
« **Confidentialité**  
(4) L’agent d’inspection assure la confidentialité de tout document, dossier ou système informatique retiré en vertu de l’alinéa 68(2)f) et de toute copie faite en vertu de l’alinéa 68(2)f). »
6. À ajouter après le paragraphe 78(3) :  
« **Confidentialité**  
(4) Le ministre des Transports assure la confidentialité de tout document, dossier ou système informatique retiré en vertu de l’alinéa 78(2)f) et de toute copie faite en vertu de l’alinéa 78(2)f). »

Enfin, nous notons également que notre [recommandation 5.1](#), qui vise à assurer que les renseignements obtenus auprès des fournisseurs de télécommunications ne soient utilisés que pour des activités de cybersécurité et d’assurance des renseignements, est pertinente pour cette section. Cette recommandation est abordée dans la section « Renforcer la responsabilité du CST » [ci-dessous](#).

## Mesure n° 3 : Maximiser la transparence

### Résumé du problème :

- **La confidentialité affaiblit la responsabilité et la régularité de la procédure :** Le projet de loi C-26 permet au ministre de prendre des arrêtés confidentiels, sans obligation de les rendre accessibles au public. S'il est compréhensible qu'un certain degré de confidentialité est nécessaire dans ce domaine, le public doit avoir une idée de la façon dont ces pouvoirs sont exercés, de leur fréquence et de leurs effets, si l'on veut que les décideurs soient tenus de rendre des comptes. Les personnes et les services indirectement touchés par le projet de loi C-26 doivent également avoir la possibilité de contester les arrêtés relatifs à la sécurité.
- **Les ordres inconnus prédominent sur la réglementation publique :** Le projet de loi C-26 donne du pouvoir à la confidentialité au point que ses arrêtés et règlements peuvent prévaloir sur des décisions prises antérieurement par des organismes de réglementation, risquant ainsi de créer une certaine confusion si ces décisions réglementaires sont publiques alors que les arrêtés relatifs à la sécurité ne le sont pas. Un tel pouvoir menace l'intégrité et l'accessibilité des cadres réglementaires du Canada et rend les règles relatives à la sécurité actuellement en vigueur inconnues du public.

### Amendements recommandés :

#### Recommandation 3.1 – Remédier au manque de dispositions en matière de transparence et de responsabilité

(Cette recommandation est rédigée selon la section 2.2 du rapport de M. Parsons)

Le projet de loi C-26 permet au gouvernement de prendre des arrêtés confidentiels applicables aux fournisseurs de télécommunications. S'il y a certainement des situations où la confidentialité peut être justifiée, elle ne devrait pas être la règle par défaut. L'obligation d'obtenir une ordonnance de la Cour fédérale constitue un moyen de contrôle et d'équilibre contre les excès du gouvernement et un moyen efficace de s'assurer que le gouvernement ne dissimule pas des actions intrusives disproportionnées :

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
<b>Non-divulgarion</b> 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.	<b>Non-divulgarion</b> 15.1(2) <del>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.</del> Le gouverneur en conseil peut présenter un avis à la Cour fédérale pour obtenir une ordonnance interdisant la divulgation du contenu du décret, en totalité ou en partie, pris en vertu du paragraphe 15.1(1). 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 du décret, en totalité ou en partie, serait préjudiciable aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité de toute personne.



<p><b>Non-divulgarion</b> 15.2(3) L'arrêté visé aux paragraphes 15.2(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.</p>	<p><b>Non-divulgarion</b> 15.2(3) <del>L'arrêté visé aux paragraphes 15.2(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.</del> Le ministre peut présenter un avis à la Cour fédérale pour obtenir une ordonnance interdisant la divulgation du contenu de l'arrêté, en tout ou en partie, pris en vertu des paragraphes 15.2(1) ou (2). 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, à la sécurité nationale ou à la sécurité de toute personne.</p>
--	---

Une situation semblable s'applique à la LPCE, qui permet au gouvernement de prendre des décrets confidentiels applicables à des exploitants désignés. Encore une fois, s'il existe certainement des situations dans lesquelles la confidentialité peut être adaptée, elle ne devrait pas être la règle par défaut. Ces modifications recommandées permettraient aux exploitants désignés de divulguer l'existence d'une directive, mais pas son contenu, sauf dans la mesure nécessaire pour se conformer à l'orientation :

<b>LPCE</b> <b>Texte original</b>	<b>LPCE</b> <b>Amendements recommandés :</b>
<p><b>Interdiction de communication</b> 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.</p>	<p><b>Interdiction de communication</b> 24 Il est interdit à tout exploitant désigné visé par une directive de cybersécurité d'en communiquer <del>l'existence ou</del> le contenu ou de permettre qu'ils le soient, sauf en conformité avec l'article 25.</p>
<p><b>Cas où la communication est permise</b> 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.</p>	<p><b>Cas où la communication est permise</b> 25(1) L'exploitant désigné visé par une directive de cybersécurité ne peut en communiquer <del>l'existence et</del> le contenu que dans la mesure nécessaire pour s'y conformer.</p>

### **Recommandation 3.2 – Les arrêtés et les décrets devraient être publiés dans la *Gazette du Canada***

*(Cette recommandation est rédigée selon la recommandation 6 de M. Parsons)*

Le projet de loi devrait être amendé pour exiger la publication des décrets ou des arrêtés dans la *Gazette du Canada* dans les 180 jours suivant leur émission ou dans les 90 jours suivant leur mise en œuvre, selon la condition qui est satisfaite en premier :

<b>Loi sur les télécommunications</b> <b>Texte original</b>	<b>Loi sur les télécommunications</b> <b>Amendements recommandés :</b>
15.1(4) Le décret est publié dans la <i>Gazette du Canada</i> , à moins que le gouverneur en conseil ne l'en ordonne autrement dans le décret.	15.1(4) Le décret est publié dans la <i>Gazette du Canada</i> , <del>à moins que le gouverneur en conseil ne l'en ordonne autrement dans le décret.</del> dans les 180 jours suivant leur émission ou dans les 90 jours suivant leur mise en œuvre, selon la condition qui est satisfaite en premier.
15.2(5) L'arrêté visé aux paragraphes 15.2(1) ou (2) est publié dans la <i>Gazette du Canada</i> , à moins que le ministre ne l'en ordonne autrement dans l'arrêté.	15.2(5) L'arrêté visé aux paragraphes 15.2(1) ou (2) est publié dans la <i>Gazette du Canada</i> , <del>à moins que le ministre ne l'en ordonne autrement dans l'arrêté</del> dans les 180 jours suivant leur émission ou dans les 90 jours suivant leur mise en œuvre, selon la condition qui est satisfaite en premier.

### **Recommandation 3.3 – Le ministre devrait être contraint de présenter des rapports concernant les arrêtés et les règlements**

*(Cette recommandation est rédigée selon la recommandation 7 de M. Parsons)*

Le projet de loi devrait être amendé de manière à obliger au ministre (ou le gouverneur en conseil pour la LPCE) de présenter un rapport annuel au Parlement. Si le ministre ne présente pas ces rapports, il devrait être tenu de se présenter devant un comité parlementaire pour expliquer ce manquement et fournir un délai dans lequel le rapport sera déposé :

**AMENDEMENT RECOMMANDÉ – *Loi sur les télécommunications* :**

1. À ajouter après le paragraphe 15.2(7) :

**Rapports**

(8) Le ministre doit déposer au Parlement un rapport annuel indiquant :

- a) le nombre d'arrêtés et de règlements pris en vertu des paragraphes 15.2(1) ou (2) au cours de l'année précédente;
- b) le nombre d'arrêtés et de règlements pris en vertu des paragraphes 15.2(1) ou (2) qui ont été abrogés au cours de l'année précédente;
- c) les types d'arrêtés ou de règlements pris en vertu des paragraphes 15.2(1) ou (2) au cours de l'année précédente;
- d) le nombre de demandes présentées à la Cour fédérale en vue d'interdire la divulgation d'un arrêté, et le nombre de demandes acceptées par la Cour;
- e) le nombre de fournisseurs de télécommunications visés par des arrêtés et des règlements pris en vertu des paragraphes 15.2(1) ou (2) au cours de l'année précédente;
- f) le nombre de fournisseurs de télécommunications qui se sont partiellement conformés aux arrêtés et aux règlements pris en vertu des paragraphes 15.2(1) ou (2) au cours de l'année précédente;
- g) le nombre de fournisseurs de télécommunication qui se sont entièrement conformés aux arrêtés et aux règlements pris en vertu des paragraphes 15.2(1) ou (2) au cours de l'année précédente;
- h) une analyse narrative de la nécessité, de la proportionnalité, du caractère raisonnable et de l'utilité des pouvoirs prévus par l'arrêté décrits aux paragraphes 15.2(1) ou (2)

(9) Si le ministre ne dépose pas ce rapport, il doit être tenu de se présenter devant un comité parlementaire pour expliquer ce manquement et fournir un délai dans lequel le rapport sera déposé.

**AMENDEMENT RECOMMANDÉ – LPCE :**

1. À ajouter après l'article 146 :

**Rapports**

(1) Le rapport doit indiquer :

- a) le nombre de directives rédigées en vertu de l'article 20 au cours de l'année précédente;
- b) le nombre de directives rédigées en vertu de l'article 20 qui ont été annulées au cours de l'année précédente;
- c) les types de directives rédigées en vertu de l'article 20 au cours de l'année précédente;
- d) le nombre d'exploitants désignés visés par des directives en vertu de l'article 20 au cours de l'année précédente;
- e) le nombre d'exploitants désignés qui se sont partiellement conformés aux directives rédigées en vertu de l'article 20 au cours de l'année précédente;
- f) le nombre d'exploitants désignés qui se sont entièrement conformés aux directives rédigées en vertu de l'article 20 au cours de l'année précédente;
- g) une analyse narrative de la nécessité, de la proportionnalité, du caractère raisonnable et de l'utilité des pouvoirs prévus par le décret décrits à l'article 20.

**Recommandation 3.4 – Les consignes du silence devraient être limitées dans le temps**

*(Cette recommandation est rédigée selon la recommandation 8 de M. Parsons)*

Le projet de loi devrait être amendé pour comprendre une période précise après la réception d'un décret, d'un arrêté ou d'un règlement, ou après leur mise en conformité, pendant laquelle un fournisseur de télécommunications ou un exploitant désigné visé par la LPCE peut communiquer qu'il a reçu un décret, un arrêté, un règlement ou une directive, ou s'est mis en conformité avec un de ces derniers :

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
<p><b>Non-divulgation</b> 15.2(3) L'arrêté visé aux paragraphes 15.2(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.</p>	<p><b>Non-divulgation</b> 15.2(3) L'arrêté visé aux paragraphes 15.2(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, <b>avant sa publication dans la Gazette du Canada. »</b></p>

<b>LPCE Texte original</b>	<b>LPCE Amendements recommandés :</b>
--------------------------------	---

<p><b>Interdiction de communication</b> 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.</p>	<p><b>Interdiction de communication</b> 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, ou jusqu'à ce que 180 jours se soient écoulés depuis l'émission de la directive de cybersécurité.</p>
---	---

**Recommandation 3.5 – Le CRTC devrait indiquer les arrêtés qui annulent des parties de ses décisions; un rapport annuel devrait indiquer le nombre de fois où des arrêtés et des règlements gouvernementaux prévalent sur les décisions du CRTC**

*(Cette recommandation est rédigée selon la recommandation 9 et 10 de M. Parsons)*

Le projet de loi devrait être amendé pour, au minimum, exiger que le Conseil de la radiodiffusion et des télécommunications canadiennes (le CRTC) publie un avis public joint à toutes ses décisions lorsqu'il y a une incompatibilité entre sa décision et un décret, un arrêté ministériel ou un règlement qui a prévalu sur une partie d'une décision du CRTC.

Le projet de loi devrait également exiger du gouvernement qu'il publie chaque année le nombre de fois où il a émis des décrets, des arrêtés ou des règlements qui ont prévalu en cas d'incohérence entre un décret, un arrêté ou un règlement donné et une décision du CRTC, et qu'il indique quelle décision du CRTC a été visée.

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
<p><b>Incompatibilité</b> 15.2(6) Les dispositions de l'arrêté pris en vertu des paragraphes (1) ou (2) l'emportent sur les dispositions incompatibles de toute décision prise par le Conseil en vertu de la présente loi, de tout autre arrêté pris en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i> ou de toute autorisation délivrée par le ministre en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i>.</p>	<p><b>Incompatibilité</b> 15.2 (6) <del>Les dispositions de l'arrêté pris en vertu des paragraphes (1) ou (2) l'emportent sur les dispositions incompatibles de</del>En cas d'incompatibilité avec toute décision prise par le Conseil en vertu de la présente loi, <del>de</del> tout autre arrêté pris en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i> ou <del>de</del> toute autorisation délivrée par le ministre en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i> :</p> <ul style="list-style-type: none"> <li>a) les dispositions de l'arrêté l'emportent sur les dispositions incompatibles de la décision;</li> <li>b) le CRTC publie un avis public joint à la décision touchée par l'incohérence;</li> <li>c) le ministre publie un rapport annuel indiquant le nombre de fois où des arrêtés pris en vertu des paragraphes 15.2(1) ou (2) ont prévalu sur les décisions du CRTC.</li> </ul>
<b>Incompatibilité</b>	<b>Incompatibilité</b>

<p>15.8(2) Les dispositions du règlement pris en vertu de l'alinéa (1)a) l'emportent sur les dispositions incompatibles de toute décision prise par le Conseil en vertu de la présente loi, de tout arrêté pris en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i> ou de toute autorisation délivrée par le ministre en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i>.</p>	<p>15.8(2) <del>Les dispositions du règlement pris en vertu de l'alinéa (1)a) l'emportent sur les dispositions incompatibles de</del>En cas d'incompatibilité entre un règlement pris en vertu de l'alinéa (1)a) et toute décision prise par le Conseil en vertu de la présente loi, <del>de</del> tout arrêté pris en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i> ou <del>de</del> toute autorisation délivrée par le ministre en vertu de la présente loi ou de la <i>Loi sur la radiocommunication</i> :</p> <ul style="list-style-type: none"> <li>a) les dispositions du règlement l'emportent sur les dispositions incompatibles de la décision;</li> <li>b) le CRTC publie un avis public joint à la décision touchée par l'incohérence;</li> <li>c) le ministre publie un rapport annuel indiquant le nombre de fois où des règlements adoptés en vertu de l'alinéa 15.8(1)a) ont prévalu sur les décisions du CRTC.</li> </ul>
--	--

### Recommandation 3.6 – Tous les règlements devraient être accessibles au Comité mixte permanent d'examen de la réglementation

(Cette recommandation est rédigée selon la recommandation 11 de M. Parsons)

Le projet de loi devrait être amendé de manière à ce que le Comité mixte permanent d'examen de la réglementation puisse obtenir, évaluer et rendre un verdict public sur tout règlement promulgué dans le cadre des projets de réforme de la *Loi sur les télécommunications* et de la LPCE. Le Comité devrait également être habilité à obtenir, évaluer et rendre un verdict public sur les règlements relatifs à la *Loi sur les télécommunications* et qui sont modifiées conformément à l'article 18 de la *Loi sur les textes réglementaires*.

<b><i>Loi sur les télécommunications</i></b> Texte original	<b><i>Loi sur les télécommunications</i></b> Amendements recommandés :
<p><b><i>Loi sur les textes réglementaires</i></b> 15.3(3) La <i>Loi sur les textes réglementaires</i> ne s'applique pas aux décrets pris en vertu de l'article 15.1 ni aux arrêtés pris en vertu de l'article 15.2.</p>	<p><b><i>Loi sur les textes réglementaires</i></b> 15.3(3) La <i>Loi sur les textes réglementaires</i> <del>ne</del> s'applique <del>pas</del> aux décrets pris en vertu de l'article 15.1 <del>et ni</del> aux arrêtés pris en vertu de l'article 15.2.</p>

LPCE Texte original	LPCE Amendements recommandés :
<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>22(1) Est soustrait à l'application des articles 3, 5 et 11 de la <i>Loi sur les textes réglementaires</i> le décret pris en vertu de l'article 20.</p>	<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>22(1) <del>Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.</del> La <i>Loi sur les textes réglementaires</i> s'applique à tous les décrets pris en vertu du paragraphe 22(1).</p>
<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>34(2) Est soustrait à l'application de la <i>Loi sur les textes réglementaires</i> tout ordre donné en vertu du paragraphe (1).</p>	<p><b>Exemption de la Loi sur les textes réglementaires</b></p> <p>34(2) <del>Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.</del> La <i>Loi sur les textes réglementaires</i> s'applique à tout ordre donné en vertu du paragraphe (1).</p>
<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>36(3) Est soustrait à l'application de la <i>Loi sur les textes réglementaires</i> tout ordre donné en vertu du paragraphe (1).</p>	<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>36(3) <del>Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.</del> La <i>Loi sur les textes réglementaires</i> s'applique à tout ordre donné en vertu du paragraphe (1).</p>
<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>43(2) Est soustrait à l'application de la <i>Loi sur les textes réglementaires</i> tout ordre donné en vertu du paragraphe (1).</p>	<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>43(2) <del>Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.</del> La <i>Loi sur les textes réglementaires</i> s'applique à tout ordre donné en vertu du paragraphe (1).</p>
<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>45(3) Est soustrait à l'application de la <i>Loi sur les textes réglementaires</i> tout ordre donné en vertu du paragraphe (1).</p>	<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>45(3) <del>Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.</del> La <i>Loi sur les textes réglementaires</i> s'applique à tout ordre donné en vertu du paragraphe (1).</p>
<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>52(2) Est soustrait à l'application de la <i>Loi sur les textes réglementaires</i> tout ordre donné en vertu du paragraphe (1).</p>	<p><b>Exemption : Loi sur les textes réglementaires</b></p> <p>52(2) <del>Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.</del> La <i>Loi sur les textes réglementaires</i> s'applique à tout ordre donné en vertu du paragraphe (1).</p>





## Mesure n° 4 : Permettre aux avocats spéciaux de protéger l'intérêt public

### Résumé du problème :

**Présentation d'éléments de preuve secrets devant les tribunaux :** même si les arrêtés relatifs à la sécurité font l'objet d'un contrôle judiciaire, le projet de loi C-26 pourrait restreindre l'accès des demandeurs aux éléments de preuve. La loi ne prend pas en compte les avocats spéciaux détenteurs d'une cote de sécurité désignés au nom des demandeurs, comme c'est le cas dans d'autres affaires liées à la sécurité nationale. Si ces dispositions constituent une solution imparfaite pour le respect d'une procédure équitable, elles offrent au moins une protection minimale des droits des demandeurs. Le projet de loi C-26 autorise même les juges à rendre des décisions selon des éléments de preuve secrets qui ne sont pas fournis, même sous forme de résumé, aux demandeurs ou à leur équipe juridique. Le projet de loi oblige même la personne visée par l'arrêté relatif à la sécurité à intenter une instance avec les coûts que cela implique.

### Amendements recommandés :

#### **Recommandation 4.1 – Créer un poste d'avocat spécial pour permettre aux éléments de preuve d'être examinés devant un tribunal de droit sans être divulgués à des tiers**

*(Cette recommandation s'appuie sur la proposition formulée dans la recommandation 12 de M. Parsons)*

Dans sa version actuelle, le projet de loi C-26 permet au ministre de présenter des éléments de preuve secrets lors d'audiences secrètes et d'exiger que leur non-divulgation. Un tel pouvoir va à l'encontre de la transparence judiciaire. Afin de trouver un juste équilibre entre la nécessité des éléments de preuve secrets et celle de la transparence judiciaire, les modifications recommandées s'inspirent de la *Loi sur l'immigration et la protection des réfugiés* et créent une fonction « avocat spécial », c'est-à-dire un avocat sélectionné par le gouvernement et bénéficiant d'une cote de sécurité très secrète, qui peut contester les éléments de preuve produits par le gouvernement en secret. De cette façon, les éléments de preuve pourront être examinés devant un tribunal de droit sans être divulgués à des parties extérieures :

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
<b>Règles</b> 15.9(1) Les règles ci-après s'appliquent aux procédures de contrôle judiciaire de tout décret pris en vertu de l'article 5.1, de tout arrêté pris en vertu de l'article 15.2 ou de tout règlement pris en vertu de l'alinéa 15.8(1)a) :	<b>Règles</b> 15.9(1) Les règles ci-après s'appliquent aux procédures de contrôle judiciaire de tout décret pris en vertu de l'article 5.1, de tout arrêté pris en vertu de l'article 15.2 ou de tout règlement pris en vertu de l'alinéa 15.8(1)a) :  a) le juge nomme une personne à partir d'une liste établie par le ministre pour agir en tant qu'avocat spécial lors de l'instance après avoir entendu les observations du demandeur et du ministre et après avoir accordé une attention et un poids particuliers aux préférences du demandeur;

<p>15.9(1)b) il lui incombe de garantir la confidentialité des éléments de preuve ou autres renseignements que lui fournit le ministre et dont la divulgation porterait atteinte, selon lui, aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui;</p>	<p>15.9(1)b) il lui incombe de garantir la confidentialité des éléments de preuve ou autres renseignements que lui fournit le ministre et dont la divulgation porterait atteinte, selon lui, aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui;</p> <p>(i) à la demande du ministre, le juge peut le dispenser de l'obligation de fournir à l'avocat spécial une copie des renseignements si le juge est convaincu que ces renseignements ne permettent pas au demandeur d'être raisonnablement informé des arguments avancés par le ministre</p> <p>(ii) pour décider s'il y a lieu d'accorder ou non une exemption au titre de l'alinéa 15.9(1)b)i), le juge peut demander à l'avocat spécial de présenter des observations et peut communiquer avec l'avocat spécial dans la mesure nécessaire pour permettre à l'avocat spécial de présenter ses observations, si le juge croit que des considérations d'équité et de justice naturelle l'exigent;</p>
	<p>À ajouter après le paragraphe 15.9(1) :</p> <p>« (i) il peut recevoir et admettre en preuve tout élément, même inadmissible en justice, qu'il estime digne de foi et utile et peut fonder sa décision sur celui-ci;</p> <p>(j) il ne doit pas fonder sa décision sur des renseignements que le ministre est exempt de fournir à l'avocat spécial, et se doit d'assurer la confidentialité de ces renseignements et les communiquer au ministre. »</p>

	<p>À ajouter après le paragraphe 15.9(3) :</p> <p><b>« Rôle de l’avocat spécial</b>  <b>(4)</b> Le rôle de l’avocat spécial est de protéger les intérêts du demandeur lors de l’instance lorsque des renseignements ou autres éléments de preuve sont entendus à huis clos et en l’absence du demandeur et de son avocat.</p> <p><b>Responsabilités de l’avocat spécial</b>  <b>(5)</b> L’avocat spécial peut contester :</p> <p>(i) l’affirmation du ministre selon laquelle la divulgation de renseignements ou d’autres éléments de preuve serait préjudiciable aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité de toute personne;</p> <p>(ii) la pertinence, la fiabilité et la suffisance des renseignements ou autres éléments de preuve produits par le ministre et non divulgués au demandeur et à son avocat, ainsi que l’importance à leur apporter.</p> <p><b>Obligation de communication</b>  <b>(6)</b> En vertu de l’alinéa 15.9(1b)i), le ministre doit, dans le délai fixé par le juge, fournir à l’avocat spécial une copie des renseignements et d’autres éléments de preuve pertinents relatifs à ses arguments, qui ont été déposés à la Cour fédérale, mais qui ne sont pas divulgués au demandeur et à son avocat ».</p>
--	--

<b>LPCE</b> <b>Texte original</b>	<b>LPCE</b> <b>Amendements recommandés :</b>
<p><b>Contrôle judiciaire : règles</b>  145(1) Les règles ci-après s’appliquent à toute requête pour contrôle judiciaire d’une directive de cybersécurité donnée en vertu de l’article 20 :</p>	<p><b>Contrôle judiciaire : règles</b>  145(1) Les règles ci-après s’appliquent à toute requête pour contrôle judiciaire d’une directive de cybersécurité donnée en vertu de l’article 20 :</p> <p>a) le juge nomme une personne à partir d’une liste établie par le ministre pour agir en tant qu’avocat spécial lors de l’instance après avoir entendu les observations du demandeur et du ministre et après avoir accordé une attention et un poids particuliers aux préférences du demandeur;</p>

<p>145(1)(b) il lui incombe de garantir la confidentialité des renseignements et autres éléments de preuve que lui fournit le ministre et dont la divulgation porterait atteinte, selon lui, à la sécurité nationale ou à la sécurité d'autrui;</p>	<p>145(1)b) il lui incombe de garantir la confidentialité des éléments de preuve ou autres renseignements que lui fournit le ministre et dont la divulgation porterait atteinte, selon lui, aux relations internationales, à la sécurité nationale ou à la sécurité d'autrui;</p> <p>(i) à la demande du ministre, le juge peut le dispenser de l'obligation de fournir à l'avocat spécial une copie des renseignements si le juge est convaincu que ces renseignements ne permettent pas au demandeur d'être raisonnablement informé des arguments avancés par le ministre;</p> <p>ii) pour décider s'il y a lieu d'accorder ou non une exemption au titre de l'alinéa 145(1)b)i), le juge peut demander à l'avocat spécial de présenter des observations et peut communiquer avec l'avocat spécial dans la mesure nécessaire pour permettre à l'avocat spécial de présenter ses observations, si le juge croit que des considérations d'équité et de justice naturelle l'exigent; »</p>
	<p>À ajouter après le paragraphe 145(1) :</p> <p>(i) il peut recevoir et admettre en preuve tout élément, même inadmissible en justice, qu'il estime digne de foi et utile et peut fonder sa décision sur celui-ci;</p> <p>(j) il ne doit pas fonder sa décision sur des renseignements que le ministre est exempt de fournir à l'avocat spécial, et se doit d'assurer la confidentialité de ces renseignements et les communiquer au ministre.</p>

À ajouter après le paragraphe 145(3) :

**« Rôle de l'avocat spécial**

(4) Le rôle de l'avocat spécial est de protéger les intérêts du demandeur lors de l'instance lorsque des renseignements ou autres éléments de preuve sont entendus à huis clos et en l'absence du demandeur et de son avocat.

**Responsabilités de l'avocat spécial**

(5) L'avocat spécial peut contester (i) l'affirmation du ministre selon laquelle la divulgation de renseignements ou d'autres éléments de preuve serait préjudiciable aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité de toute personne; (ii) la pertinence, la fiabilité et la suffisance des renseignements ou autres éléments de preuve produits par le ministre et non divulgués au demandeur et à son avocat, ainsi que l'importance à leur apporter.

**Obligation de communication**

(6) Sous réserve de l'alinéa 145(1)c)i), le ministre doit, dans le délai fixé par le juge, fournir à l'avocat spécial une copie des renseignements et d'autres éléments de preuve pertinents relatifs à ses arguments, qui ont été déposés à la Cour fédérale, mais qui ne sont pas divulgués au demandeur et à son avocat ».

## Mesure n° 5 : Renforcer la responsabilité du Centre de la sécurité des télécommunications

*Résumé du problème :*

**Pouvoirs sans responsabilité conférés au Centre de sécurité des télécommunications :** La LPCE permettrait au Centre de sécurité des télécommunications (CST), l'organisme canadien de renseignement électromagnétique étranger et de cybersécurité, d'obtenir et d'analyser des données liées à la sécurité auprès d'entreprises à qui les Canadiens confient leurs renseignements personnels les plus délicats. Cela comprendrait les banques et les coopératives de crédit sous réglementation fédérale, les fournisseurs de télécommunications et d'énergie, et même certaines agences de transport en commun. L'utilisation de ces informations par le CST n'est pas limitée à l'aspect cybersécurité de son mandat, et toute utilisation serait largement soumise à un examen après coup plutôt qu'à une surveillance en temps réel, ce qui entraînerait un manque important en matière de responsabilité démocratique.

*Amendements recommandés :*

### **Recommandation 5.1 – Les renseignements obtenus ne devraient être utilisés que pour des activités de cybersécurité et d'assurance de l'information**

*(Cette recommandation est rédigée selon la recommandation 16 de M. Parsons)*

Le projet de loi devrait être amendé pour limiter les organismes gouvernementaux à l'utilisation exclusive des renseignements obtenus auprès des fournisseurs de télécommunications en vertu du projet de loi C-26 pour les activités de cybersécurité et d'assurance de l'information. Les renseignements ne devraient pas être utilisés à des fins de renseignement d'origine électromagnétique ou étrangers, de soutien interministériel non relatif à la cybersécurité ou d'opérations cybernétiques actives ou de défense. Ces restrictions devraient s'appliquer à tous les organismes, y compris, mais sans s'y limiter, ceux qui relèvent de la compétence du ministre de la Sécurité publique et de la Protection civile.

<b>Loi sur les télécommunications Texte original</b>	<b>Loi sur les télécommunications Amendements recommandés :</b>
1. À AJOUTER après l'article 15.6 :	« 15.6(2) 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. »

<b>LPCE Texte original</b>	<b>LPCE Amendements recommandés :</b>
<b>Conseils du Centre de la sécurité des télécommunications</b> 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	<b>Conseils du Centre de la sécurité des télécommunications</b> 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

<p>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.</p>	<p>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 <i>Loi sur le Centre de la sécurité des télécommunications</i> concernant l'exercice des attributions qui lui sont conférées sous le régime de la présente loi.</p>
<p>2. À AJOUTER après l'article 23 :</p> <p>« 23.1 Tout renseignement échangé conformément à l'article 23 ne peut être utilisé que par la personne destinataire qu'aux fins prévues à l'article 5. »</p>	
<p><b>Maintien du droit de communiquer les renseignements</b></p> <p>26(2) Le présent article ne porte aucunement atteinte à la communication de renseignements confidentiels à un organisme chargé du contrôle d'application de la loi ou au Service canadien du renseignement de sécurité si la communication est par ailleurs licite.</p>	<p><b>Maintien du droit de communiquer les renseignements</b></p> <p>26(2) Le présent article ne porte aucunement atteinte à la communication de renseignements confidentiels à un organisme chargé du contrôle d'application de la loi ou au Service canadien du renseignement de sécurité si la communication est par ailleurs licite.</p> <p><b>Restriction liée à l'utilisation :</b> 26(3) Les renseignements communiqués en vertu des paragraphes (1) ou (2) doivent être utilisés qu'à des fins liées à la protection des services essentiels, des systèmes essentiels ou des cybersystèmes essentiels.</p>

En outre, nous notons que l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a, pendant deux années consécutives (2020, 2021), fait état de problèmes relatifs à l'accès aux renseignements du CST que l'organisme de surveillance utilise pour confirmer la légalité de ses activités. Il est essentiel de combler cette lacune en matière de responsabilité pour donner confiance au public dans le fait que le CST opère dans les limites de la loi. À cet égard, les députés pourraient envisager des mesures telles que l'obligation pour tous les organismes ayant fait l'objet d'un contrôle, y compris le CST, de fournir publiquement des commentaires sur la conformité ou la conformité attendue aux demandes de leurs organismes de contrôle dans un délai déterminé. Les députés pourraient également envisager que tous les arrêtés pris en vertu de l'article 15.2 de la *Loi sur les télécommunications* ou les décrets pris en vertu de l'article 20 de la *LPCE* soient accessibles à l'OSSNR.

Nous notons également, en particulier pour les députés, les recommandations suivantes de l'éminent Christopher Parsons (Ph. D.) :

- **Recommandation 24 de M. Parsons : Tout le contenu de la loi doit être clair :** Le gouvernement devrait préciser comment les menaces prévues dans le cadre du projet de loi (« notamment face aux menaces d'ingérence, de manipulation ou de perturbation ») se comparent aux actes particuliers énoncés au paragraphe 27(2) de la *Loi sur le CST* (« tout méfait, toute utilisation non autorisée ou toute perturbation »), dans le but d'expliquer si les réformes de la *Loi sur les télécommunications* élargiraient, réduiraient ou aborderaient les mêmes catégories de lois que celles prises en compte dans la *Loi sur le CST*.
- **Recommandation 25 de M. Parsons : Des définitions claires devraient être présentes dans la loi ou rendues publiques :** Le projet de loi devrait être amendé pour fournir des définitions claires des termes « ingérence », « manipulation » et « perturbation », ou pour préciser que les définitions se trouvent dans d'autres lois particulières, ou encore pour ordonner au gouvernement de partager publiquement ces définitions et toute mise à jour

ultérieure de ces définitions en dehors de la loi.



## Références et ressources

### Ressources clés

- [Texte intégral du projet de loi C-26](#)
- [Résumé législatif du projet de loi C –26](#) (Bibliothèque du Parlement)
- [Lettre conjointe de la société civile](#) (PDF) (also [in English](#))
- [Communiqué de presse de la société civile](#) (also [in English](#))
- [Citizen Lab/Rapport de Christopher Parsons \(Ph. D.\)](#): « Cybersecurity will not thrive in darkness » ([PDF](#)) (disponible en anglais uniquement)

### Couverture médiatique

- Canadian Press : « [Federal cybersecurity bill threatens privacy, transparency, civil society groups say](#) » (Jim Bronskill) (disponible en anglais uniquement)
- News Forum – Canadian Justice : « [Bill C-26, Cybersecurity & Civil Liberties](#) » (L'animatrice Christine Van Geyn interviewe Brenda McPhail [Ph. D.] [ACLC] et Rosa Addario d'OpenMedia) (disponible en anglais uniquement)
- CTV News Power Play : « [Interview with Dr Chris Parsons](#) » (disponible en anglais uniquement)
- Canadian Press : « [Liberal cybersecurity bill a 'bad law' that must be amended, research report warns](#) » (Jim Bronskill) (disponible en anglais uniquement)
- IT World Canada : « [Proposed telecom cybersecurity law gives Canadian government too much secret power: Researcher](#) » (disponible en anglais uniquement)
- Options politiques : « [Don't give CSE more powers until it submits to effective review](#) » (Christopher Parsons [Ph. D.]) (disponible en anglais uniquement)
- Hill Times : « [Canadians' privacy could take a serious hit this coming legislative session](#) » (Ken Rubin) (disponible en anglais uniquement)
- CTV News/Canadian Press : « [Mendicino open to working with MPs to 'improve' much-criticized cybersecurity bill](#) » (disponible en anglais uniquement)
- Toronto Star (article d'opinion d'OpenMedia) : « [MPs must say no to agency request for powers to spy on your bank and travel records](#) » (disponible en anglais uniquement)