Le 28 septembre 2022

À :
L'honorable Marco E. L. Mendicino, C.P., député,
Ministre de la Sécurité publique.

CC :
L'honorable François-Philippe Champagne, C.P., député,
Ministre de l'Innovation, des Sciences et de l'Industrie.

L'honorable Pierre Poilievre, C.P., député, chef de l'opposition
Yves-François Blanchet député, chef du Bloc Québécois
Jagmeet Singh, député, chef du NPD
Elizabeth May députée, chef parlementaire du Parti Vert

Lettre conjointe de préoccupation concernant le projet de loi C-26

Monsieur le Ministre,

Nous, les organisations soussignées, vous écrivons pour vous faire part de nos sérieuses préoccupations concernant 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.*

Dans votre communiqué de presse annonçant ce projet de loi, vous avez déclaré : " Au XXIe siècle, la cybersécurité est synonyme de sécurité nationale. " Nous sommes d'accord, et nous partageons votre objectif d'aider les secteurs public et privé à mieux se protéger contre les cyberattaques.

Cependant, dans sa forme actuelle, le projet de loi C-26 est profondément problématique et doit être corrigé. Tel qu'il est rédigé, il risque de porter atteinte à notre droit à la vie privée, ainsi qu'aux principes de gouvernance responsable et d'application régulière de la loi qui constituent le tissu de la démocratie canadienne. La législation doit être modifiée en profondeur pour garantir qu'elle offre des protections efficaces en matière de cybersécurité tout en préservant ces principes démocratiques essentiels.

Comme vous le savez, le projet de loi C-26 accorde au gouvernement de nouveaux pouvoirs étendus sur de vastes pans de l'économie canadienne. Nous croyons que ces pouvoirs doivent être strictement limités et accompagnés de garanties et d'exigences de rapport significatives afin que les Canadiens puissent demander des comptes à leur gouvernement et aux agences de sécurité. **En d'autres termes, à de grands pouvoirs doit correspondre une grande responsabilité.**

Dans le but d'améliorer cette législation, nous vous faisons part des préoccupations spécifiques suivantes :

- **Ouverture à des obligations de surveillance :** Le projet de loi C-26 autorise le gouvernement à ordonner secrètement aux fournisseurs de services de télécommunication « de mener ou de ne pas mener une action ». Cela ouvre la porte à des obligations de surveillance qui peuve être imposer sur les entreprise privees et des autres risques tel que normes de chiffrement affaiblies – quelque chose le publique a déjà dit n'est pas acceptable.

- **L'interruption des 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 spécifiques, et interdire à toute entreprise d'offrir ces services à d'autres, par un ordre secret du gouvernement. Cela ouvre la porte à une situation où les entreprises ou des canadiens soient coupés de services essentiels sans explication. Le projet de loi C-26 ne prévoit aucun régime explicite, comme un organisme de réglementation indépendant doté de pouvoirs robustes, pour gérer les effets collatéraux des ordonnances de sécurité du gouvernement.

- **Nuisance à la protection de la vie privée :** Le projet de loi C-26 permette le gouvernement de recueillir de vastes catégories d'informations des opérateurs désignés, dans n'importe quel délai et sous n'importe quelle condition. Cela peut permettre au gouvernement d'obtenir des renseignements personnels identifiables et dépersonnalisés et de les distribuer ensuite à des organisations nationales et peut-être étrangères.

- **Aucune mesure de protection pour restreindre l'abus :** Le projet de loi C-26 ne prévoit pas d'évaluation obligatoire de la proportionnalité, de la protection de la vie privée ou de l'équité, ni d'autres mesure de protection pour limiter les abus des nouveaux pouvoirs qu'il accorde au gouvernement - pouvoirs assortis d'amendes élevées ou même d'emprisonnement en cas de non-respect. Ces ordonnances s'appliquent à la fois aux entreprises de télécommunications et à un beaucoup d'autres entreprises et organismes sous réglementation fédérale désignés en vertu de la *loi sur la protection des cybersystèmes essentiels*. Des poursuites peuvent être engagées pour des violations présumées d'ordonnances de sécurité survenues jusqu'à trois ans auparavant.

- **Le secret nuit à la responsabilisation et à l'application régulière de la loi :** Le projet de loi C-26 permet au gouvernement d'adopter ses ordonnances de secret, sans exigences de divulgation au public. Même si un certain degré de confidentialité est nécessaire dans cette sphère, le public doit avoir une connaissance minimale de la façon dont ces pouvoirs sont utilisés, à quelle fréquence ils le sont et dans quels buts, pour tenir les décideurs responsables de leurs actions. Les personnes et les services touchés par le projet de loi C-26 doivent également avoir la possibilité de contester les ordonnances de sécurité.

- **Les décrets inconnus l'emportent sur la réglementation publique :** Le projet de loi C-26 accorde une importance si grande au secret que ses décrets et ses règlements pourraient avoir préséance sur des décisions précédemment prises par des organismes de réglementation, ce qui ferait en sorte que les lois sur la sécurité actuellement en vigueur ne seraient pas connues du public.

- **Preuves secrètes au tribunal :** Même si les ordonnances de sécurité sont soumises à un révision judiciaire, le projet de loi C-26 pourrait restreindre l'accès des demandeurs aux preuves. Le projet de loi ne prévoit pas que les avocats détenant une autorisation de sécurité puissent représenter les requérants. Bien que ces dispositions soient une solution imparfaite pour l'application régulière de la loi, elles assurent une protection minimale des droits des requérants. Le projet de loi C-26 permet même aux juges de prendre des décisions sur la base de preuves secrètes qui ne sont pas fournies, même sous forme de résumé, aux demandeurs

ou à leur équipe juridique. Il incombe également à la personne visée par une ordonnance de sécurité d'engager une révision judiciaire, avec les coûts que cela implique.

- **Des pouvoirs sans responsabilités pour le Centre de la sécurité des télécommunications (CST) :** Le projet de loi C-26 laisserait le CST – l'organisme national chargé de la cybersécurité et du renseignement électromagnétique – recueillir et analyser les données relatives à la sécurité d'entreprises réglementées par le gouvernement fédéral, auxquelles les citoyens confient leurs renseignements personnels les plus sensibles. Il s'agit notamment des banques et des coopératives de crédit sous réglementation fédérale, des fournisseurs de télécommunications et d'énergie, et même de certains organismes de transport en commun. L'utilisation de ces renseignements par le CST n'est pas limitée à l'aspect cybersécurité de son mandat, et toute utilisation de ces renseignements serait sujette à une évaluation après coup plutôt qu'une surveillance en temps réel, ce qui entraînerait un déficit important en matière de responsabilité démocratique.

- **Manque de justification :** Même si le gouvernement affirme que de nouveaux pouvoirs secrets d'une telle importance sont essentiels, il n'a pas publié de données suffisamment claires établissant la nécessité et la proportionnalité des pouvoirs proposés.

En résumé, la cybersécurité est importante et nous devons la maîtriser : Tous les résidents du Canada peuvent s'entendre sur la nécessité de la cybersécurité. Toutefois, les libertés civiles, la protection de la vie privée et la confiance dans la primauté du droit et la gouvernance responsable sont les fondements de ce sentiment de sécurité. Il est impératif que, dans ses efforts pour offrir une cybersécurité solide aux Canadiens, le gouvernement assure également la responsabilisation et le respect des droits fondamentaux.

À mesure que le projet de loi C-26 progresse dans le processus législatif, nous nous réjouissons de travailler avec vous et avec les parlementaires de tous les partis pour veiller à ce qu'il assure une cybersécurité solide pour tous les Canadiens, tout en garantissant la responsabilisation et le respect de nos droits.

Sincèrement,

Association canadienne des libertés civiles
Fondation canadienne de la Constitution
Coalition pour la surveillance internationale des libertés civiles
Leadnow
Ligue des droits et libertés
OpenMedia
Conseil du Canada de l'accès et la vie privée

Christopher Parsons, associé de recherche principal au Citizen Lab, école Munk, Université de Toronto
Tamir Israel, avocat spécialisé dans les droits numériques
Andrew Clement, professeur émérite, Faculté d'information, Université de Toronto

Envoyé mercredi 28 septembre par OpenMedia au nom des organisations et des personnes susmentionnées.