Ashar S. Ahmed, B. Sc., M. Sc., SSCP, CC

Le 24 octobre 2024

Sénateur Tony Dean
Président, Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants (SECD)
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Sénateur Jean-Guy Dagenais
Vice-président, Comité SECD
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Objet : Besoin urgent d'adopter le projet de loi C-26 pour renforcer la cybersécurité et améliorer la prestation des services publics

Messieurs les Sénateur Dean et Dagenais,

Je vous écris en espérant que vous êtes tous deux en pleine santé. Je vous écris en tant que praticien américano-canadien de la sécurité des systèmes et de la cybersécurité ayant une expérience antérieure dans notre service public en matière de cybersécurité, préoccupé par l'état actuel de la situation en matière de sécurité numérique au pays.

Le discours au sujet du projet de loi C-26 a été marqué par des désaccords et des controverses, en grande partie en raison des préoccupations concernant la centralisation potentielle du pouvoir et les problèmes de protection de la vie privée qui pourraient découler de sa promulgation. En tant que professionnel fortement impliqué dans le secteur de la cybersécurité, j'ai la ferme conviction que l'importance de l'adoption de cette législation dépasse de loin ces préoccupations.

Une cyberattaque se produit dans le monde toutes les 39 secondes, ce qui souligne l'urgence de renforcer nos défenses contre ces menaces, dont la complexité et le potentiel de nuisance ne cessent de croître. La cybersécurité n'est pas simplement un problème localisé pour les économies

technologiquement développées; c'est un problème mondial, et le Canada **doit** être à l'avant-garde de la lutte contre ce problème.

La création récente du ministère de la Cybersécurité et des Solutions numériques en Nouvelle-Écosse[1] reflète le besoin croissant de services rapidement réactifs, efficacement adaptés et pratiques.

La création de ce ministère est un premier pas dans la transformation de la prestation de services et dans l'amélioration de la cybersécurité dans la province, exploit que le projet de loi C-26 peut imiter à l'échelle fédérale.

Toutefois, il est essentiel que toutes les parties s'engagent dans un dialogue collaboratif, trouvent un terrain d'entente et répondent aux préoccupations tout en maintenant l'esprit de la loi. Pour répondre à ces préoccupations tout en préservant l'esprit et les objectifs du projet de loi C-26, j'ai proposé une série de modifications qui s'articulent autour des principes suivants :

Pouvoirs autorisés : Cet aspect permet au ministre ou à un fonctionnaire désigné, en consultation avec le Centre de la sécurité des télécommunications Canada (CST), d'ordonner à un fournisseur de services de télécommunications de prendre des mesures précises pour rendre le système canadien de télécommunications plus sécuritaire. Cela donne au gouvernement le pouvoir nécessaire tout en maintenant des garanties contre les ingérences indues.

Normes de protection des données : La modification proposée met l'accent sur le respect des lois canadiennes existantes en matière de protection des données, telles que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE*)*, ce qui devrait atténuer les préoccupations relatives à la protection des renseignements personnels et au mauvais usage des données.

Transparence et responsabilité : Les dispositions exigeant des explications écrites pour les ordonnances, des consultations avec les parties prenantes et des résumés publics renforcent le sens des responsabilités et devraient dissiper les craintes de concéder un pouvoir illimité.

Procédure d'appel : La modification proposée prévoit une procédure d'appel auprès de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), qui

[1] *Le nouveau ministère se concentrera sur les services et les programmes numériques. Gouvernement de la Nouvelle-Écosse*, **https://novascotia.ca/news/release/?id=20230524001** [DISPONIBLE EN ANGLAIS SEULEMENT].

constituerait un contrôle essentiel de l'autorité gouvernementale et garantirait que les ordonnances sont justifiables et proportionnées.

En conclusion, je vous implore, ainsi que tous les membres du Comité permanent de la sécurité publique et nationale, de vous concentrer sur l'importance cruciale du projet de loi C-26 pour la cybersécurité de notre pays et la prestation de services publics. Les risques de retarder ou de diluer cette législation sont bien trop grands. Je vous invite à prendre en considération mes suggestions et à travailler avec diligence pour parvenir à un consensus qui permettra de renforcer la sécurité numérique et d'améliorer la prestation de services pour tous les Canadiens.

Je vous remercie de votre temps et de votre attention. J'ai la conviction que, sous votre direction, notre pays s'orientera vers un avenir numérique sûr et efficace.

Respectueusement,

Ashar S. Ahmed, B. Sc., M. Sc., SSCP, CC
Sécurité des systèmes/Praticien de la cybersécurité

Ordonnance
Début du bloc inséré
(2) Le ministre, ou un fonctionnaire désigné autorisé par le ministre, peut, en consultation avec le Centre de la sécurité des télécommunications Canada (CST), par ordonnance, ordonner à un fournisseur de services de télécommunications de faire quelque chose ou de s'abstenir de faire quelque chose - autre qu'une chose énoncée dans le paragraphe (1) ou 15. 1(1) - qui est précisée dans l'ordonnance et qui est, de l'avis du ministre ou du fonctionnaire désigné, nécessaire pour assurer la sécurité du système canadien de télécommunications, notamment contre les menaces d'ingérence, de manipulation ou de perturbation. Dans l'ordonnance, le ministre ou le fonctionnaire désigné peut notamment.

(a) interdire à un fournisseur de services de télécommunications d'utiliser un produit ou un service déterminé dans son réseau ou ses installations de télécommunications, ou en relation avec ceux-ci, ou toute partie de ces réseaux ou installations;

…

(l) exiger d'un fournisseur de services de télécommunications qu'il mette en œuvre des normes précises en ce qui concerne ses services, réseaux ou installations de télécommunications.

Normes de protection des données
(5) En collaboration avec le CST, le ministre ou le fonctionnaire désigné veille à ce que la gestion des renseignements obtenus des fournisseurs de services de télécommunication respecte les normes de protection des données conformément aux lois canadiennes existantes en la matière, notamment la LPRPDE.

Transparence et responsabilité
(4) Le ministre ou le fonctionnaire désigné assure la transparence et la responsabilité du processus de prise de décision en :

(a) fournissant une explication écrite de la raison d'être de l'ordonnance, y compris une évaluation des risques, des avantages et de l'incidence sur le fournisseur de services de télécommunications concerné;

(b) réexaminant et mettant à jour régulièrement l'ordonnance afin de s'assurer qu'elle reste nécessaire et proportionnée par rapport à l'objectif;

(c) consultant les parties intéressées, y compris le fournisseur de services de télécommunications concerné, avant d'émettre ou de modifier l'ordonnance, sauf si cela risque de compromettre l'objectif de l'ordonnance;

(d) divulguant publiquement un résumé de l'ordonnance, sous réserve des limitations nécessaires pour protéger les renseignements confidentiels et les préoccupations en matière de sécurité nationale.

Procédure d'appel

(3) Un fournisseur de services de télécommunications peut faire appel d'une ordonnance prise en vertu du paragraphe (2) auprès de l'OSSNR en tant que conseil d'examen indépendant. L'OSSNR est habilité à examiner l'ordonnance, à entendre le ministre ou le fonctionnaire désigné et le fournisseur de services de télécommunications concerné, et à déterminer si l'ordonnance est justifiée selon les preuves présentées, tout en tenant compte des exigences en matière de transparence et de responsabilité. L'OSSNR rendra une décision dans un délai déterminé et sa décision sera contraignante.

Fin du bloc inséré