



Le 24 octobre 2024

Objet : Étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, par le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants

Mesdames et Messieurs les membres du comité,

Au nom de ses membres du secteur de l'assurance IARD, le Bureau d'assurance du Canada (BAC) souhaite profiter de cette occasion pour commenter le projet de loi C-26, qui, s'il est adopté, édictera la *Loi sur la protection des cybersystèmes essentiels* (la « LPCE »).

Le BAC est l'association sectorielle nationale qui représente les sociétés privées d'assurance résidentielle, automobile et commerciale au Canada. Nos membres constituent l'essentiel du marché de l'assurance multirisque privée au Canada. Depuis plus de 50 ans, le BAC collabore avec les gouvernements et les organismes de réglementation du secteur de l'assurance à l'échelle du pays en vue de rendre l'assurance habitation, automobile et commerciale abordable pour tous les Canadiens.

Les cybermenaces grandissantes ont contribué à la croissance du marché de l'assurance au Canada.

En 2023, les primes de cyberassurance ont atteint 550 millions de dollars, ce qui en fait l'un des produits d'assurance les plus recherchés et à la croissance la plus rapide au Canada¹. Dans un contexte mondial de plus en plus marqué par l'incertitude géopolitique, la menace de cyberattaques étrangères contre des infrastructures essentielles s'intensifie, ce qui devrait accroître le besoin en assurance cybersécurité au cours des prochaines années.

Il faut apporter un amendement ciblé pour permettre aux exploitants d'infrastructures nationales essentielles d'accéder à la cyberassurance nécessaire.

Le BAC appuie généralement l'application des exigences du projet de loi C-26 aux exploitants d'infrastructures essentielles, car cela correspond aux objectifs de l'industrie, qui sont de renforcer la cybersécurité des infrastructures essentielles nationales au Canada. Le BAC estime toutefois que, si la loi était adoptée sous sa forme actuelle, elle pourrait compromettre la capacité des exploitants d'infrastructures nationales essentielles à respecter les obligations contractuelles de leurs polices d'assurance, lesquelles exigent la communication des changements importants liés aux risques afin de maintenir une couverture de cyberassurance.

Le paragraphe 20(1) permet au gouverneur en conseil, par décret, de 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. L'article 24

¹BAC, avec des données de MSA Research Inc.



interdit à tout exploitant désigné visé par une directive de cybersécurité d'en communiquer l'existence, sauf dans le cas des exceptions précises énoncées à l'article 25.

Un changement important lié aux risques s'entend de tout changement dans les activités d'un assuré qui modifierait sensiblement son profil de risque. **Sous sa forme actuelle, la LPCE n'indique pas clairement si un exploitant désigné qui est soumis à une directive de cybersécurité serait en mesure de divulguer à son assureur un changement connu important lié aux risques découlant d'une directive de cybersécurité.**

Dans tout contrat d'assurance, on trouve une clause qui oblige les assurés à signaler à leur assureur tout changement important lié aux risques. Les assureurs exigent d'être informés rapidement des changements importants liés aux risques afin qu'ils puissent évaluer les risques avec précision et les gérer, ajuster les prix, prévenir la fraude, se conformer aux lois et, enfin, maintenir l'intégrité des contrats d'assurance.

Si la LPCE empêche les assurés d'informer leur assureur d'un changement connu et important en matière de risque, elle pourrait avoir pour conséquence négative involontaire de rendre plus restrictives les exigences de souscription dans ce secteur. Ce resserrement des conditions résulterait de deux facteurs : les assureurs auraient du mal à évaluer avec précision les cyberrisques associés aux infrastructures essentielles, et les couvertures d'assurance risqueraient davantage d'être compromises en raison de l'incapacité ou du défaut de l'exploitant désigné de communiquer à son assureur les changements importants liés au risque attribuables à une directive de cybersécurité.

Compte tenu de l'élargissement de la définition des infrastructures essentielles et de l'introduction de nouveaux cyberrisques, nous sommes d'avis que l'amendement suivant aiderait considérablement à atténuer les conséquences néfastes potentielles pour le marché de la cyberassurance, les infrastructures essentielles et, en fin de compte, la cybersécurité canadienne. Vous trouverez ci-après une proposition de modification mineure de l'article 25 de la LPCE (en rouge).

Amendement proposé

Cas où la communication est permise

25. (1) L'exploitant désigné visé par une directive de cybersécurité ne peut en communiquer l'existence et le contenu que dans la mesure nécessaire pour s'y conformer.

Interdiction : communication subséquente

(2) Nul ne peut communiquer des renseignements obtenus au titre du paragraphe (1) ou permettre qu'ils le soient sans l'autorisation de l'exploitant désigné.

Droit de communiquer un changement important lié aux risques

(3) **L'article 24 n'a pas pour effet d'empêcher un exploitant désigné d'informer son assureur d'un changement connu important lié aux risques qui découlerait d'une directive de cybersécurité.**

À notre avis, l'amendement ci-dessus clarifierait la LPCE en permettant explicitement aux assurés de communiquer à leur assureur tout changement important lié aux risques lorsque le changement en question découle d'une directive de cybersécurité, ce qui éliminerait ainsi les conséquences indésirables potentielles du projet de loi tel qu'il est actuellement rédigé.



Il est important de noter que le BAC ne demande pas un amendement qui permettrait ou exigerait qu'un exploitant désigné assuré divulgue à son assureur l'émission d'une directive de cybersécurité ou la teneur d'une telle directive. Le BAC souhaite simplement confirmer que le projet de loi ne vise pas à empêcher un exploitant désigné assuré de communiquer à son assureur un changement important lié aux risques qui découlerait d'une directive de cybersécurité.

Nous croyons que cet amendement ciblé permettrait d'éviter cette conséquence négative et involontaire importante. Le marché de la cyberassurance pourrait ainsi continuer d'évaluer avec précision la couverture d'assurance contre les cyberattaques afin de répondre à la demande croissante des exploitants d'infrastructures nationales essentielles.

Je vous remercie de l'attention que vous porterez à cette question. Nous nous tenons à votre disposition pour vous apporter toutes les précisions nécessaires.

Si vous souhaitez obtenir de plus amples informations ou poser des questions concernant le présent mémoire, veuillez communiquer avec :

Jason Clark, directeur national, Changements climatiques et enjeux fédéraux

JClark@ibc.ca