IEDM Des idées pour une société plus prospère

LE POINT

COLLECTION RÉGLEMENTATION

DÉCEMBRE 2022

PROJET DE LOI C-26 : LES RISQUES D'UNE MICROGESTION DE LA CYBERSÉCURITÉ

Par Célia Pinto Moreira

Compte tenu de l'importance croissante que les technologies numériques revêtent dans nos vies quotidiennes, il est crucial d'assurer la sécurité de nos données informatiques. Dans cette optique, le gouvernement canadien a présenté le projet de loi C-26 (PL C-26)[1] contenant la *Loi sur la protection des cybersystèmes essentiels* (LPCE), qui réglementera les cybersystèmes essentiels privés tombant sous la supervision fédérale[2] et prévoira de lourdes pénalités en cas de non-conformité. Or, plutôt que de protéger les systèmes de cybersécurité des entreprises privées, l'approche adoptée risque de les bureaucratiser et de les pénaliser.

UN CARCAN ADMINISTRATIF

Si la LPCE est adoptée, on constituera une liste des entreprises qui ont des cybersystèmes jugés essentiels dans plusieurs secteurs clés tels que les télécommunications et le secteur bancaire. Ces entreprises auront 90 jours pour établir un programme de cybersécurité et le fournir à l'organisme réglementaire responsable de leur secteur[3].

Le programme devra, du moins sur papier au moment de l'examen, cerner et gérer les risques de cybersécurité et prévenir toute « compromission » ou tout incident de cybersécurité[4]. Par la suite, les entreprises devront faire réexaminer leur programme annuellement et informer l'organisme responsable de toute modification apportée.

La LPCE impose aussi des sanctions administratives pécuniaires si une quelconque obligation n'est pas respectée. Les pénalités, qui selon la *Loi* « vis[ent] non pas à punir mais à favoriser le respect de la présente loi[5] », peuvent aller jusqu'à 15 millions de dollars[6].

Toutefois, il est à craindre qu'au lieu de mener à une meilleure cybersécurité, la mise en place d'un tel carcan administratif, assorti de sanctions pécuniaires substantielles, entraîne plutôt une aversion des entreprises privées à prendre des initiatives qui vont au-delà des exigences légales minimales. En effet, pourquoi vous donner la peine de prendre de nouvelles mesures pour protéger les consommateurs si votre programme a déjà été approuvé, et que cela risque de vous compliquer la vie et de vous exposer à des sanctions à hauteur de millions de dollars en cas de non-approbation?

LES ENTREPRISES PRIVÉES VEILLENT DÉJÀ À LA CYBERSÉCURITÉ

Les entreprises canadiennes n'ont pas attendu le PL C-26 pour se préoccuper de la cybersécurité. Elles ont déjà des programmes en place, et elles ont collectivement dépensé près de 10 milliards de dollars en détection et en prévention des incidents de cybersécurité en 2021, une augmentation de 41 % – soit de 2,8 milliards de dollars – par rapport à 2019[7] (voir la Figure 1).

Par exemple, dans le secteur des télécommunications, certains opérateurs ont mis en place une stratégie innovante qui vise à trouver « un équilibre entre des protections proactives et la préparation face aux pires scénarios » dans l'anticipation des incidents[8]. D'autres opérateurs ont été reconnus comme des leaders internationaux en matière de cybersécurité, notamment grâce à l'intégration

de différentes technologies permettant d'amasser beaucoup de données sur les menaces potentielles tout en respectant les désirs des clients[9].

Il en va de même dans le secteur bancaire, où 93 % des PDG considèrent la cybersécurité comme la principale motivation pour investir dans des stratégies diverses et variées[10]. Ces stratégies incluent notamment une collaboration entre les banques canadiennes[11] et l'embauche de hackers « éthiques » qui testent en continu la cybersécurité[12] des établissements.

Ainsi, si les pouvoirs publics peuvent définir les contours et les grandes lignes d'un cadre de cybersécurité, ils n'ont certainement pas l'expertise des entreprises privées pour microgérer leurs programmes de cybersécurité.

UNE MICROGESTION CONTREPRODUCTIVE

Une instance réglementaire qui vérifierait tous les aspects des programmes de cybersécurité privés et où tout changement devrait être approuvé rajouterait inévitablement une couche de lourdeur réglementaire au processus. Or, cela risque d'avoir l'effet opposé de celui recherché, car dans un domaine comme la cybersécurité, où les attaques se déroulent rapidement et changent sans cesse de forme, les entreprises privées ne peuvent se permettre de voir leur prise de décision ralentie par des considérations d'ordre bureaucratique; elles ont plutôt besoin de réagir vite, sans obstacle administratif.

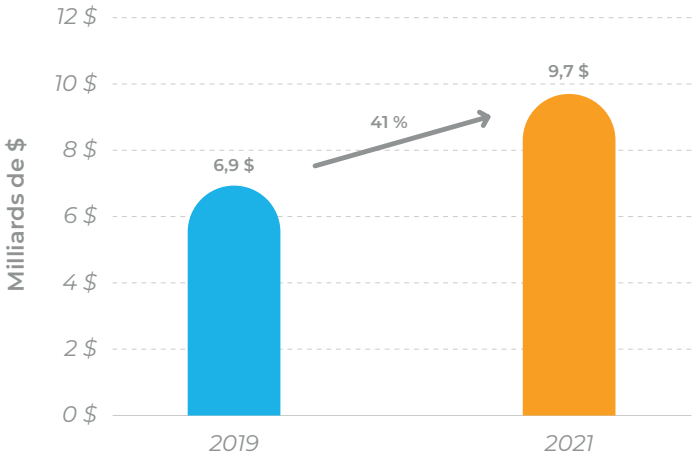
La panne de Rogers à l'été 2022 est un bon exemple, illustrant comment les entreprises privées réagissent et peuvent par elles-mêmes assurer la sécurité de leurs clients. Après une mise à jour de ses systèmes, Rogers a été victime d'une panne où son service a été interrompu pendant plusieurs heures, ce qui a privé de nombreuses personnes de services critiques comme Interac[13] ou encore l'accès au 911[14].

Pour éviter que cela se reproduise, les entreprises du secteur des télécommunications ont conclu un accord d'entraide en cas de future panne à grande échelle[15]. La réaction n'aurait pas été aussi rapide si des instances réglementaires avaient entravé la réactivité des entreprises.

La cybersécurité est un enjeu réel dans lequel le gouvernement fédéral a sans doute un rôle à jouer, notamment dans les cas de cyberterrorisme d'État. Mais tel l'arbitre qui ne dicte pas aux équipes comment se passer la rondelle pour la mettre au fond du filet, le gouvernement devrait à tout prix éviter de microgérer les programmes de cybersécurité des entreprises privées.

Figure 1

Évolution des dépenses des entreprises canadiennes en détection et en prévention des incidents de cybersécurité



Source : Calculs de l'auteure. Statistique Canada, « L'incidence du cybercrime sur les entreprises canadiennes, 2021 », *Le Quotidien*, 18 octobre 2022.

RÉFÉRENCES

1. Imran Ahmad *et al.*, « Projet de loi C-26 : l'importance accrue de la cybersécurité au Canada », Norton Rose Fulbright, 22 juin 2022.
2. PL C-26, annexe 1.
3. Imran Ahmad *et al.*, *op. cit.*, note 1.
4. PL C-26, Édiction de la loi, Établissement d'un programme de cybersécurité.
5. PL C-26, Édiction de la loi, Sanctions administratives pécuniaires.
6. Shane Morganstein, Julie M. Gauthier et Daniel J. Michaluk, « Projet de loi C-26 : nouvelle loi canadienne sur la cybersécurité des infrastructures essentielles », Borden Ladner Gervais, 20 juin 2022.
7. Statistique Canada, « L'incidence du cybercrime sur les entreprises canadiennes, 2021 », *Le Quotidien*, 18 octobre 2022.
8. Cogeco, Placer nos clients au cœur de nos activités, Sécurité des données, consulté le 28 novembre 2022.
9. Bell Canada, *Aligning cybersecurity with market dynamics and customer needs*, octobre 2019, p. 4 et 16.
10. PricewaterhouseCoopers, « Canadian Banks Collaborate to Combat Cyber Risks », communiqué de presse, 6 mars 2018.
11. *Idem*.
12. The Canadian Press, « Canadian banks hire "ethical hackers" to improve and test cybersecurity », CBC News, 22 novembre 2018.
13. Plan Hub, « Panne Rogers 2022 », PlanHub.ca, 19 juillet 2022.
14. Radio-Canada, « Entretien avec Éric Parent : fragilité des nombreux réseaux au pays », *Tout un matin*, 12 juillet 2022.
15. The Canadian Press, « Rogers outage: Telecoms reach deal to "ensure" services in emergencies », Global News, 7 septembre 2022.

Ce Point a été préparé par **Célia Pinto Moreira**, analyste en politiques publiques à l'IEDM. La Collection Réglementation de l'IEDM vise à examiner les conséquences souvent imprévues pour les individus et les entreprises de diverses lois et dispositions réglementaires qui s'écartent de leurs objectifs déclarés.

910, rue Peel, bureau 600, Montréal (Québec) H3C 2H8 T 514.273.0969
150, 9e Avenue SW, bureau 2010, Calgary (Alberta) T2P 3H9 T 403.478.3488
iedm.org