De : Responsable Acces
A : [redacted]
Objet : Demande d"information | Dossier 2023-11437
Date : 12 décembre 2023 09:20:43
Pièces jointes : [redacted]

[redacted]

[redacted]

La présente donne suite à votre demande d'accès à l'information reçue le 22 novembre 2023, laquelle est rédigée ainsi :

> « J'aimerais obtenir tous les échanges (messages, courriels, documents, communications, études, rapports et-ou autres) entre l'entreprise chinoise Huawei et le ministère ces cinq dernières années. »

Conformément à l'article 47 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) (« Loi sur l'accès »), nous vous informons que le ministère des Finances détient des documents correspondant à votre demande.

Vous trouverez, ci-joint, une lettre ainsi qu'un rapport transmis par Huawei (45 pages). Veuillez noter que le rapport est également disponible en ligne, à l'adresse : https://www-file.huawei.com/-/media/corporate/Local-site/ca/images/2021/cyber-security-and-data-privacy__fr.pdf

Si vous désirez contester cette décision, il vous est possible de le faire en vous adressant à la Commission d'accès à l'information dans les trente (30) jours suivant la date de la présente décision. Vous trouverez ci-joint une note explicative concernant l'exercice de ce recours.

Je vous prie de recevoir, [redacted], l'expression de mes sentiments distingués.

David St-Martin
Directeur général
Responsable de l'accès aux documents
et de la protection des renseignements personnels

Direction générale de l'organisation du budget,
de l'administration et du secrétariat
Ministère des Finances
390, boulevard Charest Est, 8e étage
Québec (Québec) G1K 3H4
Tél.: 418 643-1229
www.finances.gouv.qc.ca

HUAWEI

L'honorable Eric Girard, MAN
Assemblée nationale du Québec
Hôtel du Parlement
1045, rue des Parlementaires
Québec (Québec) G1A 1A3

Le 21 mai 2021

Ministre Girard,

Huawei Canada est le principal fournisseur d'équipements qu'utilisent les réseaux de télécommunications du pays. À titre de partenaires de confiance des compagnies de télécommunications du Canada, nous souhaitons rassurer les Canadiens quant à la sécurité de leurs données. Comme nous l'avons fait tout au long de nos 13 années de prestation de services au Canada, nous demeurons résolus à respecter tous les tests, normes et règlements qui sont exigés et à maintenir notre historique d'absence d'intrusion dans notre réseau, tout en précisant qu'aucune incidence de quelque problème que ce soit n'a été signalée.

À cet égard, vous trouverez ci-joint un récent rapport intitulé *Cybersécurité et protection des données personnelles : Considérations clés pour les décideurs publics* qu'a publié un important cabinet-conseil d'envergure internationale, Roland Berger. Ce rapport couvre le paysage politique et fait état d'opinions concernant l'orientation future des besoins du gouvernement en matière de politiques dans ce domaine. Il indique les étapes qui seraient requises dans le but de réduire les menaces à la cybersécurité. Elles comprennent la mise en place de normes simples ainsi qu'une bonne reddition de comptes de la part de toutes les entreprises qui oeuvrent au sein du marché canadien.

Depuis le début de nos activités au Canada en 2008, Huawei Canada s'est consacré à fournir à ses clients un service qui soit uniquement de la plus haute qualité. Nos recherches en matière de technologie ont permis de définir Huawei Canada comme un partenaire fier, fiable et transparent dont les investissements en recherche et développement ont hissé l'entreprise au rang des 20 principaux investisseurs qui soutiennent l'écosystème canadien d'innovation, grâce à des investissements de 261 millions $ en 2019 incluant deux centres de recherche à Montréal et à Québec.

À titre de leader politique ayant de l'intérêt envers ce domaine, nous désirons partager directement avec vous ce Rapport. Si vous avez quelque question concernant son contenu ou tout autre sujet, nous serions plus qu'heureux d'en discuter avec vous.

Nous vous remercions du temps que vous voudrez bien nous consacrer.

Nous vous prions d'agréer, l'expression de nos sentiments les meilleurs.

Steve Liu
Vice-Président des affaires publiques et communications

HUAWEI TECHNOLOGIES CANADA CO., LTD.
+1 (416) 518-0256
liuwei44259@huawei.com

12 YEARS / ANS IN / AU CANADA
CONNECTING THE UNCONNECTED
UNE CONNEXION POUR TOUS

HUAWEI
TECHNOLOGIES CANADA CO., LTD.
19 Allstate Parkway, 4th Floor,
Markham, ON L3R 5A4, Canada
Tel: 1-905-944-5000
Fax: 1-905-944-5027
www.huawei.com

Cybersécurité et protection des données personnelles

Considérations clés pour les décideurs publics

Janvier 2021

HUAWEI

Roland Berger

Avis de non-responsabilité générale

Ce rapport a été élaboré uniquement par Roland Berger et a été commandé par Huawei. Le rapport se fonde sur des informations accessibles au public, qui n'ont pas été vérifiées de manière indépendante par RB, ainsi que sur des entretiens avec plusieurs acteurs clés du marché, tels que des sociétés de télécommunications et d'autres entreprises du secteur des TIC, sur certaines hypothèses, des évaluations générales, des projections et l'expérience tirée des activités de conseil de RB, dans chaque cas au moment de la préparation du rapport.

Toutes les hypothèses, évaluations, points de vue, projections et valeurs d'expérience contenus dans ce rapport impliquent des éléments importants de jugement et d'analyse subjectifs, qui peuvent ou non être corrects. Bien que les informations contenues dans ce rapport soient considérées comme exactes, ni RB, ni aucune de ses filiales, partenaires, employés ou agents ne fournissent de garantie, expresse ou implicite, ni n'acceptent de responsabilité ou d'obligation au cas où les développements futurs réels différeraient des déclarations et des projections contenues dans ce rapport. Aucune partie de ce document ne peut être utilisée ou invoquée par une personne ou une organisation, et Roland Berger n'assume aucune responsabilité et ne peut être tenu responsable de toute perte ou dommage résultant d'une telle utilisation ou invocation.

TABLE DES MATIÈRES

SOMMAIRE EXÉCUTIF

Avec l'émergence des infrastructures digitales, de nombreuses transactions économiques et sociales sont de plus en plus numérisées. Les banques en ligne, les réseaux sociaux, les réseaux électriques intelligents et les réseaux industriels sont des exemples d'activités qui reposent désormais largement sur les données numériques. En effet, la quantité et la vitesse à laquelle les données numériques sont générées et stockées ne cessent d'augmenter, et ce, de manière exponentielle. Si la plupart des données sont insignifiantes, une quantité importante contient des informations sensibles et doit être protégée. Ainsi, des mesures importantes de cybersécurité doivent être adoptées pour garantir l'intégrité de l'économie numérique et la confidentialité des données privées.

Du point de vue de la cybersécurité, les menaces proviennent d'acteurs externes et internes dont les capacités s'améliorent constamment. À mesure que les organisations adoptent les transactions numériques, elles s'engagent dans une transformation de leur modèle d'affaires. Cependant, dans de nombreux cas, elles ne disposent pas d'experts à l'interne pour protéger les données des clients et des transactions. Ainsi, les Canadiens n'ont jamais été aussi touchés par la cybercriminalité. Les taux de signalement de cybercrimes, y compris ceux liés à la fraude et aux vols d'identité, augmentent de façon spectaculaire. Les infrastructures critiques telles que les réseaux d'électricité ou d'aqueduc sont également de plus en plus menacées.

Du point de vue de la protection des données personnelles, la numérisation accrue des transactions commerciales et des interactions sociales crée de nouvelles opportunités pour les cybercriminels de voler des données leur permettant d'exploiter des informations personnelles ou critiques à des fins de fraude, d'espionnage et de sabotage. Bien que les réglementations relatives à la protection des données doivent être modernisées pour s'adapter aux nouvelles technologies, elles ne doivent pas entraver l'innovation numérique ni bloquer la mise en œuvre de ces nouvelles technologies. Cette dichotomie entre l'innovation numérique et la protection des données personnelles alimente donc le débat sur la quantité de réglementation nécessaire dans le cyberespace.

La crise sanitaire de la COVID-19 et d'autres tendances telles que la recherche constante d'efficacité continueront à favoriser l'adoption de la technologie numérique dans les transactions quotidiennes des consommateurs et les opérations commerciales des institutions. L'économie sera ainsi davantage exposée à la cybercriminalité. Le coût total de la cybercriminalité dans le monde est actuellement estimé à 525 milliards de dollars US, soit environ 0,7% du PIB mondial, et devrait augmenter si les mesures appropriées ne sont pas prises. Ce ratio est plus élevé dans les régions développées et est indicatif de la nécessité pour des pays tels que le Canada de prendre des mesures importantes dans ce domaine.

Les décideurs publics ne peuvent pas négliger l'importance de leur rôle dans la mise en place d'un environnement numérique sûr permettant de préserver la confiance du public envers les nouvelles technologies et de soutenir la croissance de l'économie numérique. La plupart des industries profitent des gains d'efficacité découlant de la numérisation – la protection des données des entreprises et des particuliers est donc essentielle au développement d'une économie compétitive.

La cybersécurité et la protection des données personnelles sont des enjeux complexes. Toutefois, en redoublant d'efforts pour résoudre les sept défis clés suivants, les décideurs publics s'attaqueraient aux problèmes les plus importants liés à la cybersécurité et à la protection des données personnelles et créeraient de meilleures conditions pour la croissance de l'économie numérique:

CYBERSÉCURITÉ

1. Améliorer la littéracie numérique du grand public
2. Soutenir les petites institutions dans leur transformation numérique
3. Sécuriser les infrastructures critiques et les réseaux gouvernementaux
4. S'adapter à l'évolution de l'environnement technologique
5. Renforcer les efforts policiers contre la cybercriminalité

PROTECTION DES DONNÉES PERSONNELLES

6. Équilibrer la protection des données personnelles et la croissance de l'économie numérique
7. Naviguer dans la complexité du paysage législatif international

L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ

Comme la plupart des composantes de la société moderne dépendent désormais fortement des services numériques, les individus et les institutions sont de plus en plus exposés aux risques de la cybercriminalité. En effet, la quantité de données générées et stockées en ligne augmente d'année en année de manière exponentielle et représente une opportunité toujours plus grande pour les cybercriminels. Le recours aux services numériques tels que les réseaux sociaux, les plateformes de commerce électronique et les services bancaires numériques augmente radicalement le nombre de vulnérabilités potentielles et permet ainsi une augmentation des cas de vol, de fraude et d'extorsion de données.

Le Canada, avec les États-Unis, est l'un des pays les plus ciblés en ce qui concerne le vol de données numériques. Le coût de la cybercriminalité en Amérique du Nord représente 0,8 % du PIB, ce qui est supérieur à la moyenne mondiale de 0,7 % (Gemalto, 2018). L'importance des gains financiers potentiels, combinés à un faible taux de réussite des services de police dans l'identification et la poursuite des cybercriminels, alimentent l'augmentation mondiale des activités de cybercriminalité.

Bien que les différents paliers de gouvernement aient pris des mesures pour améliorer en général la cybersécurité du Canada, la situation exige toujours une attention constante. Des vols de données importants et très médiatisés, comme ceux de Capital One et de Desjardins, se produisent fréquemment. De plus, de nombreuses cyberattaques visant les petites entreprises, les grandes institutions et les fournisseurs d'infrastructures essentielles restent souvent non détectées, non signalées ou confidentielles.

La sécurisation de l'infrastructure numérique est donc de la plus haute importance pour assurer la confiance du public et favoriser l'adoption des technologies. Il s'agit d'un pilier essentiel pour soutenir la croissance de l'économie numérique du Canada. Comme la plupart des industries bénéficient des gains d'efficacité découlant du numérique, la protection des données des entreprises et des particuliers est essentielle pour assurer la compétitivité future du Canada.

La cybersécurité doit être abordée sur plusieurs fronts. Pour atténuer l'impact de la cybercriminalité, nous pensons que les décideurs publics canadiens devraient se concentrer sur cinq grands défis :

1. Améliorer la littératie numérique du grand public ;
2. Soutenir les petites institutions dans leur transformation numérique ;
3. Sécuriser les infrastructures critiques et les réseaux gouvernementaux ;
4. S'adapter à l'évolution de l'environnement technologique ;
5. Renforcer les efforts policiers contre la cybercriminalité.

En relevant ces cinq défis, les décideurs publics s'attaqueront à la plupart des problèmes clés dans le domaine de la cybersécurité et offriront de meilleures conditions pour soutenir la croissance de l'économie numérique. Ces défis ont été établis sur la base de l'état actuel de la cybercriminalité et du paysage politique canadien qui soutient les efforts en cybersécurité.

2.1 PORTRAIT DE LA CYBERCRIMINALITÉ

La cybercriminalité a évolué au fil du temps et, pour en comprendre l'état actuel, il est essentiel d'identifier les acteurs à l'origine des attaques ainsi que leurs motivations, les tactiques employées et leurs cibles. Cette mise en contexte est nécessaire pour comprendre les menaces auxquelles le Canada est actuellement confronté.

2.1.1 Acteurs

Les cyberattaques contre les organisations proviennent généralement d'acteurs externes (voir figure 2.1). Cependant, les fuites provenant d'acteurs internes, tels que les employés et les partenaires commerciaux, sont disproportionnellement fréquentes en Amérique du Nord par rapport au reste du monde. Elles représentent environ 30 % des fuites de données signalées aux États-Unis et au Canada, contre seulement 16 % dans le reste du monde (Verizon, 2020).

Les acteurs internes ont parfois des intentions malveillantes, mais ils ne sont généralement pas conscients des répercussions de leurs actions, et ce, en raison d'un manque de formation et de connaissance de base en technologie. Des employés sont régulièrement victimes d'hameçonnage ou partagent simplement par inadvertance des informations avec les mauvaises personnes. Le taux plus élevé au Canada de fuites de données dues à des acteurs internes est indicatif de la vulnérabilité des systèmes informatiques canadiens à la mauvaise littéracie numérique des employés manipulant ou ayant accès à des informations sensibles.

D'autre part, les acteurs externes sont de plus en plus sophistiqués et sont souvent soutenus par des organisations criminelles ou étatiques. Le crime organisé et les États représentent respectivement environ 70 % et 10 % des acteurs externes signalés, bien que cette distinction soit parfois difficile à établir en raison de la coopération entre certains acteurs étatiques et non étatiques. Les 20 % restants sont principalement constitués d'acteurs non affiliés dont les motivations demeurent souvent floues (Verizon, 2020).

Figure 2.1 – Description des principaux acteurs de la cybercriminalité

	Acteurs	Description	Exemples d'objectifs
Acteurs externes	**Cyberterroristes**	**Groupes extrémistes** utilisant l'informatique pour intimider, forcer un changement politique ou provoquer la peur ou des dommages physiques	› Perturber les infrastructures critiques › Modifier ou supprimer les dossiers de renseignement des terroristes connus
	Acteurs étatiques	**Groupes hautement sophistiqués** recevant des conseils, un financement ou une assistance technique de la part d'un état	› Faciliter l'espionnage étatique › Utiliser l'information volée comme levier pour obtenir d'autres types de renseignements
	Cybercriminels	**Des individus ou des groupes organisés malveillants** accédant à des données personnelles ou financières pour les monétiser	› Frauder ou faire des vols d'identité › Récolter des listes de renseignements et les utiliser pour des attaques d'hameçonnage
	Hacktivistes	**Groupes organisés** cherchant à sensibiliser à une cause ou à exercer la liberté d'expression	› Publier une brèche pour mettre en évidence les vulnérabilités d'une organisation › Recueillir des informations sur une cible
	Amateurs de sensations fortes	**Des individus cyniques et opportunistes** accédant à des systèmes protégés pour le défi que cela représente	› Revendiquer une cyberattaque réussie › Gagner en crédibilité auprès d'une communauté virtuelle
Acteurs internes	**Menaces internes**	**Les personnes qui opèrent déjà au sein d'organisations** commettant ou facilitant une cyberattaque, parfois involontairement (par exemple, des employés mécontents, opportunistes ou mal formés)	› Vendre les données confidentielles des clients ou la propriété intellectuelle › Divulguer les messages des dirigeants d'entreprises privées

Source : Centre canadien pour la cybersécurité, RAND Corporation, recherche documentaire, Roland Berger

2.1.2 Motifs

Le gain financier est le principal motif de la grande majorité des cyberattaques visant les particuliers et les institutions. Pour les entreprises, environ 90 % des vols de données sont motivés par un gain financier direct. Le reste est principalement lié à l'espionnage industriel visant des secteurs hautement techniques (Verizon, 2020). Parmi les autres motivations, on peut citer l'activisme, la satisfaction personnelle et la notoriété.

Pour les particuliers, l'hameçonnage ou le piratage des informations personnelles est généralement effectué dans le but d'obtenir un gain financier. D'autres motifs pour les vols d'informations personnels sont les tentatives d'atteinte à la réputation ou d'ingérence électorale, qui sont généralement parrainées par des États.

2.1.3 Tactiques

Les tactiques les plus courantes utilisées par les cybercriminels peuvent être classées en quatre grands groupes : le piratage, l'ingénierie sociale, l'exploitation des erreurs des utilisateurs et les logiciels malveillants.

- **Le piratage** fait souvent référence à des attaques par force brute, au cours desquelles les cybercriminels tentent de trouver par essais et erreurs des combinaisons de mots de passe ou des pages web cachées. Le piratage fait également référence à la simple utilisation d'identifiants volés obtenus sur le marché noir ou grâce à d'autres tactiques de cyberattaque. Environ 80 % des attaques de piratage utilisent soit la force brute soit des identifiants volés. Le reste utilise différentes vulnérabilités nécessitant certains niveaux de sophistication (Verizon, 2020)
- **Les tactiques d'ingénierie sociale** font principalement référence à des campagnes d'hameçonnage au cours desquelles les cybercriminels envoient une grande quantité de courriels ou de SMS, en se faisant passer pour une institution légitime et en demandant des informations personnelles. Par exemple, pendant la crise de la COVID-19, les cybercriminels se sont fait passer pour l'Agence canadienne du revenu et ont convaincu des individus à divulguer leurs informations personnelles et bancaires. Ils ont ainsi pu détourner des paiements de la Prestation canadienne d'urgence (PCU).
- **L'exploitation des erreurs des utilisateurs** repose sur la mauvaise configuration des outils de stockage d'infonuagique et d'autres outils accessibles au public, ou sur la transmission accidentelle d'informations sensibles, généralement par le biais de courriels envoyés aux mauvais destinataires.
- **Les logiciels malveillants** existent sous de nombreuses formes, mais consistent généralement en des programmes installés par inadvertance sur les appareils des utilisateurs, souvent par le biais de pièces jointes ou de liens malveillants dans les courriers électroniques. Les programmes invisibles conçus pour capturer et transmettre des mots de passe ou d'autres informations sensibles sont les formes de logiciels malveillants les plus répandues. Les logiciels d'extorsion sont un autre type de logiciels malveillants courants. Ils menacent de publier ou de détruire des données à moins qu'une rançon ne soit versée. Les logiciels d'extorsion sont de plus en plus courants depuis l'essor des cryptomonnaies puisque celles-ci permettent des méthodes de paiement intraçables et facilitent le blanchiment des profits de la cybercriminalité.

L'exploitation des erreurs des utilisateurs et les tactiques d'ingénierie sociale deviennent les tactiques les plus répandues, remplaçant peu à peu les logiciels malveillants. Ce changement est dû au nombre croissant d'utilisateurs avec une mauvaise littéracie numérique, et est causé par l'adoption de plus en plus large des technologies numériques. En outre, l'amélioration des standards de cybersécurité a rendu inefficaces de nombreux anciens logiciels malveillants.

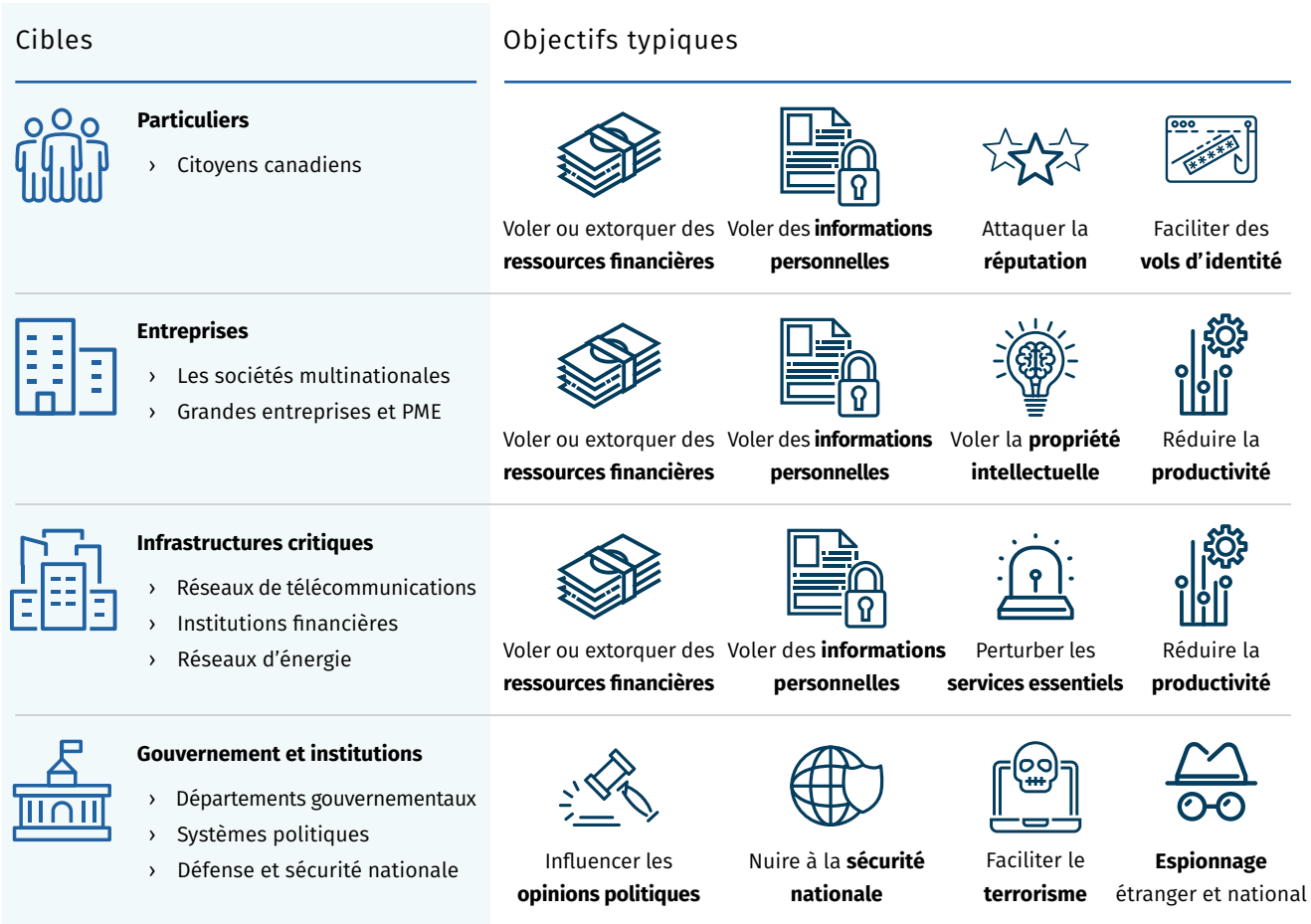
2.1.4 Cibles

La cybercriminalité vise tous les acteurs de la société numérique : les particuliers et les entreprises, les infrastructures critiques et les réseaux gouvernementaux.

- **Les citoyens canadiens** sont de plus en plus pris pour cible par les cybercriminels. Les cybercrimes signalés ont augmenté de plus de 20 % par an depuis 2014 (Statistique Canada, 2019). La quantité importante d'information volée au cours des dernières années rend assez simple pour les cybercriminels l'accumulation suffisante d'informations personnelles sur certains individus pour commettre des fraudes ou des vols d'identité. La mauvaise littéracie numérique de certains utilisateurs permet également aux criminels d'utiliser des tactiques d'ingénierie sociale peu sophistiquées et d'exploiter leurs erreurs pour obtenir des informations d'identification ou d'autres informations sensibles.

- Pour les **entreprises canadiennes**, le coût moyen d'une brèche informatique est estimé à environ 6 millions de dollars canadiens, soit environ 15 % de plus que la moyenne mondiale de 5,3 millions de dollars canadiens (IBM Security / Ponemon Institute, 2019). Le coût moyen par dossier volé est plus élevé au Canada, malgré un nombre inférieur de dossiers volés par infraction. Il est important de noter que bien que les entreprises de toutes tailles soient touchées par la cybercriminalité, les petites entreprises sont souvent plus vulnérables en raison de leurs faibles ressources en cybersécurité.
- L'effort de digitalisation de nombreuses **infrastructures critiques**[1] pour gagner en efficacité ouvre la porte aux cyberattaques. Les attaques sont souvent menées par des acteurs étatiques confirmés ou suspectés, et exemplifient la possibilité d'une cyberguerre coordonnée. Par rapport à d'autres pays, les infrastructures critiques du Canada n'ont pas été particulièrement affectées par des cyberattaques. Néanmoins, le secteur de la santé a été mis à l'épreuve ces dernières années, subissant de multiples attaques par des logiciels d'extorsion et des fuites d'information. Le nombre total d'attaques contre les infrastructures critiques reste cependant inconnu. Les attaques qui échouent ne sont communiquées qu'aux autorités compétentes, car une divulgation publique serait contre-productive.
- **Les réseaux gouvernementaux** sont une cible de choix pour le vol de données. Ils stockent souvent de grandes quantités de données de haute qualité et, comme leurs opérations sont souvent essentielles et financées par des fonds publics, ils peuvent être des cibles particulièrement intéressantes pour des logiciels d'extorsion. Au Canada, les institutions gouvernementales ont pris des mesures importantes ces dernières années pour protéger leurs réseaux, mais l'évolution rapide des cybermenaces exige une mise à jour constante et exigeante des mesures de sécurité. Les petites institutions publiques, telles que les municipalités rurales et de taille moyenne, deviennent particulièrement vulnérables en raison de leur manque de ressources en matière de cybersécurité.

Figure 2.2 – Vue d'ensemble des cibles et des objectifs types



Source : Roland Berger

1. Les fournisseurs d'infrastructures essentielles comprennent les services publics, les télécommunications, la finance, les soins de santé, l'eau, l'alimentation, les transports, la sécurité publique et les industries manufacturières essentielles.

2.2 APERÇU DU PAYSAGE POLITIQUE CANADIEN EN MATIÈRE DE CYBERSÉCURITÉ

La cybersécurité relève principalement de juridiction fédérale en raison de sa nature nationale et souvent internationale. Les provinces qui disposent de leur propre service de police – l'Ontario, le Québec et Terre-Neuve-et-Labrador – sont responsables de l'application de la législation sur la cybercriminalité, pour autant que l'affaire ne dépasse pas les frontières provinciales ou nationales. Étant donné que les cyberattaques se propagent facilement au-delà des frontières provinciales et internationales, il est facile de comprendre pourquoi les enquêtes sur les cybercrimes de grande envergure relèvent la plupart du temps de la GRC.

Au Canada, la cybersécurité est réglementée et régie par un cadre complexe de ministères et d'organismes fédéraux. Comme le montre la figure 2.3, trois ministères différents (la Sécurité publique, le Conseil du Trésor et la Défense nationale) supervisent les organismes chargés de la lutte contre la cybercriminalité.

Figure 2.3 – Séparation fédérale actuelle des responsabilités en matière de cybersécurité

Sécurité publique

- Formule et soutient la mise en œuvre de la stratégie nationale de cybersécurité
- Coordonne les efforts de cybersécurité avec les acteurs nationaux et internationaux

Gendarmerie royale du Canada

- Enquête les cybercrimes au niveau national
- Coordonne avec les services de police des partenaires internationaux

Conseil du Trésor

- Supervise l'élaboration et la mise en œuvre, à l'échelle du gouvernement, de mesures de cybersécurité appropriées

Services partagés Canada

- Consolide et gère la plupart des infrastructures informatiques des ministères du gouvernement fédéral

Défense nationale

- Soutient les efforts de recherche et de développement des secteurs public et privé dans le domaine de la cybersécurité des infrastructures critiques

Établissement de sécurité canadien

- Gère le CCC

Service canadien du renseignement de sécurité

- Évalue les cyber-menaces nationales et internationales

Centre canadien pour la cybersécurité (CCC)

- Réunit la plupart des compétences fédérales en matière de cybersécurité au sein d'une seule organisation
- Prévient, identifie et atténue l'impact des cyberattaques sur les réseaux gouvernementaux, les infrastructures critiques, les entreprises et les citoyens
- Soutient les efforts de la GRC grâce au Groupe national de coopération en matière de cybercriminalité (GNC3)

La structure ci-dessus n'inclut pas les entités actives dans le domaine de la confidentialité des données, comme le Commissariat à la protection de la vie privée. Les détails du cadre de protection de la vie privée au niveau fédéral sont présentés dans la section 3.

Aperçu de la stratégie de cybersécurité

La stratégie et le plan d'action actuels du gouvernement fédéral, publiés respectivement en 2018 et 2019, s'articulent autour de trois axes principaux: la sécurité et la résilience des réseaux canadiens, le soutien à l'innovation en cybersécurité et le rôle de chef de file du gouvernement fédéral.

- Le premier axe se concentre principalement sur la protection des réseaux du gouvernement fédéral et de ceux des infrastructures critiques, notamment dans les secteurs financier et énergétique. Le gouvernement vise à améliorer ses capacités de détection et de collecte de renseignements et à collaborer davantage avec les fournisseurs d'infrastructures critiques. Les capacités de la GRC ont également été renforcées grâce à des ressources supplémentaires et à la création du Groupe nationale de coordination contre la cybercriminalité (GNC3) en collaboration avec le Centre canadien pour la cybersécurité (CCC).
- Pour soutenir l'innovation en cybersécurité, le gouvernement fédéral se concentre sur le développement de la main-d'œuvre nécessaire dans ce domaine, par le biais d'un programme de placement professionnel financé, et sur le soutien des mesures de sécurité des PME, en mettant en place un nouveau programme de certification leur étant dédié. Le Canada soutient également les efforts de recherche, tant dans les institutions publiques que dans le secteur privé, par le biais du financement fourni par le nouveau Programme de coopération en matière de cybersécurité et par les organismes conventionnels de financement de la recherche du ministère de l'Innovation, des Sciences et du Développement Économique (ISDE), tels que le Conseil National de Recherches du Canada (CNRC) et le Conseil de Recherches en Sciences Naturelles et en Génie (CRSNG).
- Enfin, le plan d'action vise à améliorer la position de chef de file du gouvernement canadien sur la scène nationale et internationale.
  - Au niveau national, le gouvernement a unifié, en 2018, toute son expertise dans une seule organisation par la création du Centre canadien pour la cybersécurité (CCC). Le CCC coordonne tous les efforts en matière de cybersécurité. Il surveille les réseaux canadiens et internationaux de cybercriminalité, informe les institutions publiques, les entreprises et les citoyens sur les menaces cybernétiques, et fournit des recommandations aux acteurs de l'économie numérique. La CCC est l'autorité fédérale sur les aspects techniques de cybersécurité et le point de contact pour tous les organismes et partenaires afin de coordonner les interventions en cas d'incident.
  - Sur la scène internationale, le Canada vise à coopérer spécifiquement avec les États-Unis en établissant un cadre mondial pour la lutte contre la cybercriminalité. Le Canada a également l'intention d'accroître sa collaboration avec ses voisins du Sud pour la mise en place de défenses de cybersécurité, notamment pour les infrastructures critiques communes (par exemple dans le secteur de l'énergie).

La stratégie canadienne actuelle aborde de nombreuses questions de cybersécurité, mais plusieurs défis demeurent. Les cinq principaux défis présentés dans les sections qui suivent ont été identifiés par l'analyse de la situation de la cybersécurité au Canada. En les adressant adéquatement, le Canada pourrait mieux protéger son environnement digital et ainsi favoriser la croissance de son économie numérique.

2.3 DÉFI 1 – AMÉLIORER LA LITTÉRACIE NUMÉRIQUE DU PUBLIC EN MATIÈRE DE CYBERSÉCURITÉ

2.3.1 Contexte

Les cybercriminels s'appuient de plus en plus sur le manque de connaissances du grand public en matière de cybersécurité pour perpétrer leurs attaques. Lorsqu'ils tentent d'infiltrer le réseau d'une entreprise, ils n'ont souvent besoin que d'un seul point d'entrée, potentiellement offert par un seul employé tombant victime d'hameçonnage ou téléchargeant par inadvertance un logiciel malveillant. Ces dernières années, les cybercriminels ont peaufiné l'exploitation de ces cibles faciles. Tel que mentionné dans la section 2.1, environ 30 % des brèches à la cybersécurité des entreprises nord-américaines proviennent d'acteurs internes. Ces brèches sont le plus souvent involontaires et sont rendues possibles par le manque de connaissances en matière de cybersécurité. En fait, le manque de littéracie numérique est une cause majeure du niveau toujours croissant de fraude, d'extorsion et de vol d'identité.

2.3.2 Considérations clés pour les politiques futures

Le manque de connaissances du public en matière de cybersécurité doit être abordé selon deux axes: les campagnes de sensibilisation et la formation.

Des campagnes médiatiques de grande envergure devraient viser à informer le public des meilleures pratiques en matière de cybersécurité. L'efficacité de ces campagnes devrait également être mesurée et contrôlée afin de s'assurer qu'elles aient un impact réel. Depuis 2011, le CCC mène la campagne Pensez cybersécurité, qui communique des conseils et des informations sur les récentes menaces cybernétiques qui touchent les Canadiens. Cette campagne pourrait être étendue afin d'améliorer les pratiques de cybersécurité d'une plus grande partie de la population. Par exemple, l'actuel Mois de la sensibilisation à la cybersécurité est une initiative gouvernementale qui met la cybersécurité au premier plan grâce à de grandes campagnes de sensibilisation et à la présence d'experts en cybersécurité dans les médias. Cette initiative devrait être élargie pour toucher une plus grande proportion de la population et développer la littératie numérique. Faire équipe avec des associations du secteur privé (par exemple, le secteur financier) pour exposer les conséquences des comportements négligents en matière de cybersécurité et mettre en évidence les meilleures pratiques contribuerait à la portée et à l'efficacité de cette initiative.

Par ailleurs, la formation concernant le traitement des informations sensibles par les employés devrait être soutenue dans les secteurs public et privé. Dans le secteur public, cette formation devrait aller au-delà du gouvernement fédéral et cibler les petites institutions, telles que les administrations municipales et les organismes de santé. Dans le secteur privé, des outils devraient être proposés aux employeurs, en particulier aux PME, pour leur permettre d'améliorer les connaissances de leur personnel en matière de cybersécurité. Le CCC, qui possède déjà l'expertise nécessaire et fournit des conseils de haut niveau aux institutions publiques et privées, est un candidat idéal pour diriger ces initiatives.

Diverses associations soutiennent déjà les efforts de sensibilisation à la cybersécurité. Par exemple, le groupe de travail antihameçonnage (APWG[2]), une association industrielle internationale regroupant de grandes entreprises de TIC et des fournisseurs de services de cybersécurité, soutient déjà le mois de sensibilisation à la cybersécurité et pourrait participer à des campagnes plus importantes. L'APWG comprend des entreprises impliquées dans les services de paiement en ligne, comme Interac et PayPal, et dans le commerce électronique, comme Amazon, qui bénéficieraient grandement d'une amélioration des comportements en matière de cybersécurité.

LE CAS DU ROYAUME-UNI
SOUTENIR LA FORMATION DES EMPLOYÉS PAR UN PROGRAMME DE CERTIFICATION DES COURS DE CYBERSÉCURITÉ ET UNE FORMATION DE BASE GRATUITE

Le Royaume-Uni a identifié le manque de sensibilisation aux menaces cybernétiques comme une lacune majeure de sa cybersécurité nationale. Ainsi, pour améliorer la cybersécurité dans le secteur privé, le centre national de cybersécurité du Royaume-Uni (NCSC[3]), l'équivalent britannique du CCC, soutient la formation des employés. Le NCSC propose un programme de certification qui permet aux entreprises d'identifier facilement les services de formation de qualité respectant les normes rigoureuses établies par le NCSC. Les programmes de formation certifiés sont compilés sur le site web du NCSC comme une référence facile pour les responsables de la cybersécurité qui cherchent à améliorer la sensibilisation et la connaissance de leur personnel. En outre, le NCSC propose également un programme de formation gratuit conçu pour les PME afin de sensibiliser les employés aux risques de cyberattaques et aux mesures de base à prendre pour se défendre contre les tactiques les plus courantes.

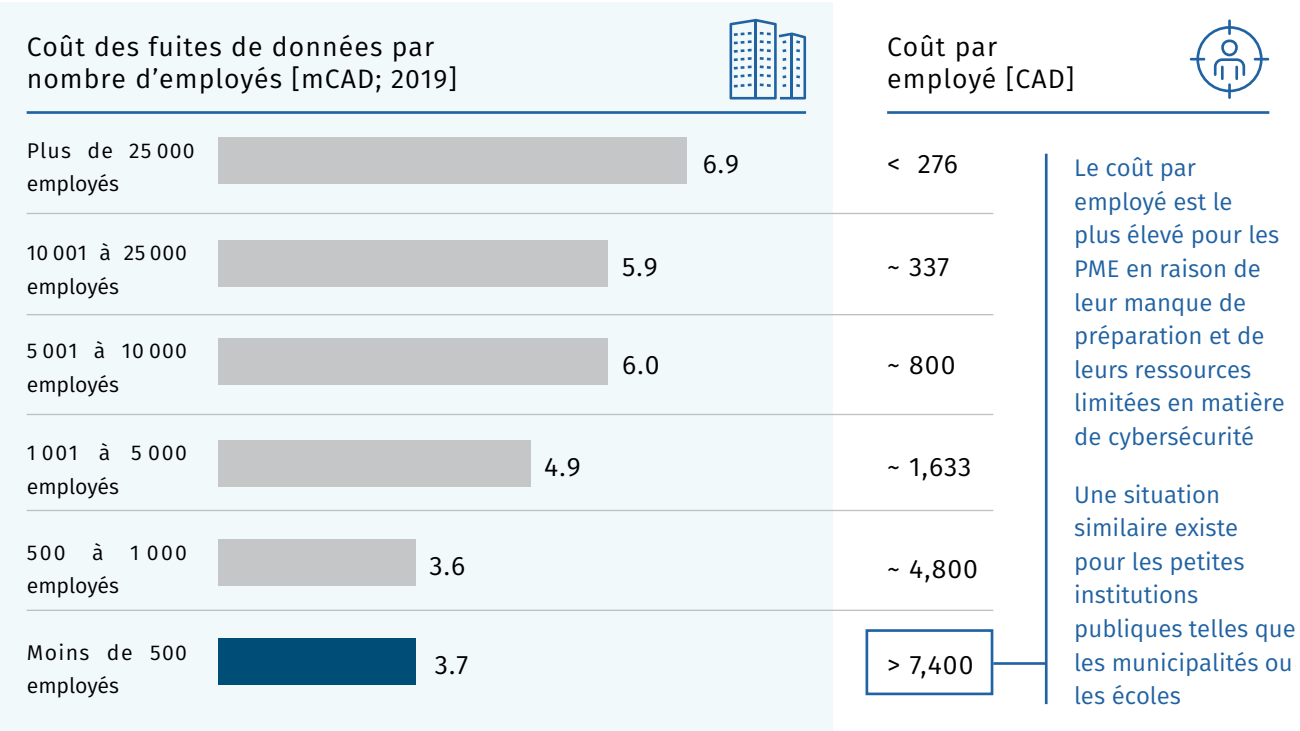
2. De l'anglais "Anti-Phishing Working Group"
3. De l'anglais "National Cyber Security Centre"

2.4 DÉFI 2 – SOUTENIR LES PETITES INSTITUTIONS DANS LEUR TRANSFORMATION NUMÉRIQUE

2.4.1 Contexte

Bien que les cyberattaques touchent les entreprises et les institutions publiques de toutes tailles, leur impact est particulièrement important pour les PME et les petites administrations publiques telles que les écoles et les petites municipalités. En effet, le coût des vols de données par employé, présenté dans la figure 2.3, est le plus élevé pour les petites entreprises. Cela s'explique par le fait que les PME ont des ressources limitées à consacrer à la cybersécurité et n'ont souvent pas les compétences nécessaires pour lutter contre les cyberattaques. Ce problème est particulièrement préoccupant pour l'économie canadienne, où le secteur privé est composé en majorité de PME, 55 % des employés canadiens travaillant dans des entreprises de moins de 500 salariés (Statistique Canada, 2019).

Figure 2.4 – Coût moyen des vols de données selon la taille des entreprises [mCAD ; 2019]



Source : IBM Security / Ponemon Institute, Roland Berger

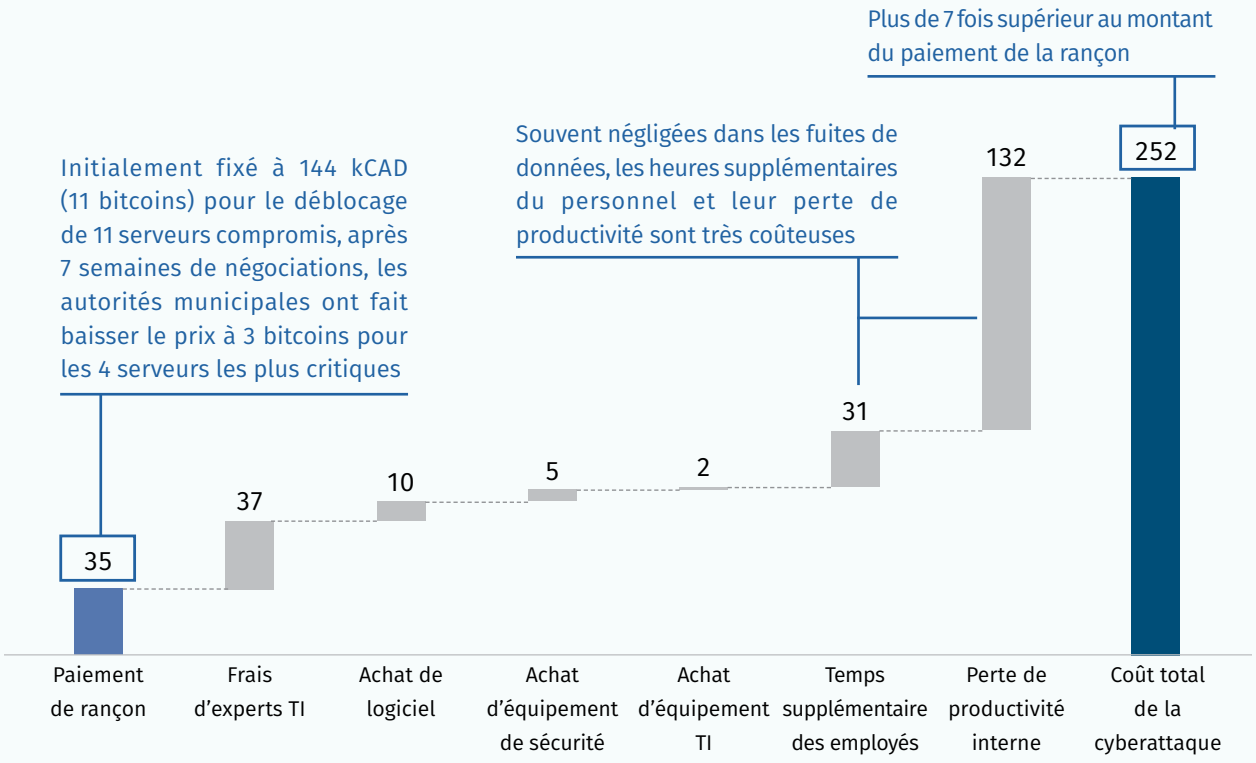
Une situation similaire existe pour les petites institutions publiques, car elles ont généralement des capacités limitées en matière de cybersécurité. Au Canada, de nombreux cas d'extorsion ou d'hameçonnage affectant des municipalités ont été exposés dans les médias. En 2019, Woodstock (ON), Stratford (ON), Ottawa (ON) et Saskatoon (SK) ont été victimes de tels incidents. De plus, il y a probablement de nombreuses autres attaques contre des municipalités qui n'ont pas été signalées ou détectées, étant donné qu'il n'existe pas de loi obligeant à signaler les incidents d'extorsion ou d'hameçonnage – seuls les vols de données doivent être signalés.

Les PME ou les petites institutions publiques estiment souvent qu'elles ne sont pas une cible potentielle pour les cybercriminels, ce qui explique une part de leur manque précaution et prise de mesures en cybersécurité. La couverture médiatique des cyberattaques se limite généralement aux fuites de données majeures qui touchent d'importantes proportions de la population. Cela renforce l'impression que les petites organisations ne sont pas ciblées, ce qui n'est malheureusement pas le cas.

COÛTS GLOBAUX DES CYBERATTAQUES

Le coût total des cyberattaques pour les petites institutions est souvent bien plus élevé que le seul coût direct d'une rançon ou d'un paiement par hameçonnage. La figure 2.4 présente une décomposition du coût total d'un incident de demande de rançon à Wasaga Beach, une petite municipalité d'Ontario, et montre comment le coût total a été sept fois plus élevé que le simple paiement de la rançon.

Figure 2.5 – Décomposition du coût total de l'incident lié à la demande de rançon de 2018 à Wasaga Beach, en Ontario [kCAD]



Source : Centre canadien pour la cybersécurité, Roland Berger

2.4.2 Considérations clés pour les politiques futures

La réponse actuelle du gouvernement du Canada à la question des cyberattaques contre les petites institutions est la création d'un programme d'évaluation et de certification dédié aux PME. Le programme de certification CyberSécuritaire Canada a été créé par Innovation, Science et Développement économique Canada (ISDE) en collaboration avec des organismes de certification existants. Bien que ce programme aide les dirigeants de PME à orienter le développement de leur infrastructure informatique vers la cybersécurité, il n'offre que peu de soutien direct. Le Canada pourrait s'inspirer du programme pour la cybersécurité des petites entreprises de l'Australie pour bonifier son support aux PME.

CAS DE L'AUSTRALIE
SOUTENIR LE COÛT DES EXAMENS DE CYBERSÉCURITÉ POUR LES PME

En raison de la vulnérabilité des PME aux cyberattaques, le gouvernement australien a mis en place un programme de financement pour soutenir les services-conseils de cybersécurité. Ce programme encourage les propriétaires d'entreprises à se renseigner sur leurs vulnérabilités et à obtenir des conseils d'experts sur la manière d'y remédier. Le programme rembourse une partie des coûts des fournisseurs de services de cybersécurité certifiés par un organisme gouvernemental, le Council of Registered Ethical Security Testers.

Les gouvernements devraient également encourager et soutenir la migration des petites institutions, publiques ou privées, vers des services d'infonuagique gérés et sécurisés. Ces dernières années, les services d'infonuagique ont permis aux PME d'étendre leurs capacités numériques et de bénéficier facilement de moyens de défense efficaces en matière de cybersécurité. En fait, ces services sont généralement fournis par de grandes entreprises dont les compétences en matière de cybersécurité sont bien supérieures à celles de la plupart des petites institutions. En migrant vers des services gérés d'infonuagique, les PME et les petites institutions publiques peuvent bénéficier de cette expertise sans avoir à constituer une solide équipe interne de cybersécurité.

Les petites entreprises canadiennes expriment déjà leur volonté d'être accompagnées dans la mise en œuvre de nouvelles mesures de cybersécurité, comme en témoigne la campagne de sensibilisation lancée en 2019 par la Canadian Advanced Technology Alliance (CATA), dont les membres sont majoritairement des PME.

2.5 DÉFI 3 – SÉCURISER LES INFRASTRUCTURES CRITIQUES ET LES RÉSEAUX GOUVERNEMENTAUX

2.5.1 Contexte

Les fournisseurs d'infrastructures critiques adoptent de plus en plus les technologies numériques pour améliorer le suivi et la gestion opérationnelle en temps réel. Cette recherche d'une efficacité accrue et de capacités supplémentaires ouvre la porte à davantage de cyberattaques. La connexion des systèmes de contrôle industriel (SCI) à l'Internet permet aux opérateurs de mieux surveiller et contrôler leurs infrastructures physiques à partir de n'importe quel endroit et à tout moment. Toutefois, elle donne aux cybercriminels la possibilité de nuire considérablement aux infrastructures en cas de brèche de sécurité. Construits pour durer, ces systèmes de contrôle fonctionnent souvent sur d'anciens logiciels qui peuvent être particulièrement vulnérables aux nouvelles cyberattaques.

Ces dernières années, de nombreux exemples internationaux ont prouvé l'efficacité des attaques contre les infrastructures critiques connectées et le risque qu'elles représentent pour la sécurité nationale. Par exemple, une coupure de courant coordonnée en Ukraine a privé 225 000 citoyens d'électricité et a paralysé les capacités de l'opérateur du réseau électrique à régler la situation. Le Canada a réussi à éviter de telles situations jusqu'à maintenant, mais n'a pas été épargné par des incidents de moindre ampleur, néanmoins dommageables. De nombreux hôpitaux et réseaux de soins de santé à travers le pays ont été touchés par des logiciels d'extorsion notoires tels que WannaCry et Ryuk. L'augmentation de l'utilisation des dossiers numériques dans les soins de santé a apporté des gains d'efficacité importants dans ce secteur, mais a rendu les activités quotidiennes vulnérables aux cyberattaques.

2.5.2 Considérations clés pour les politiques futures

La protection des infrastructures d'information critiques (IIC) est l'un des éléments clés de la stratégie et du plan d'action actuels en matière de cybersécurité. Le gouvernement fédéral vise à fournir des évaluations de cybersécurité des réseaux d'IIC ainsi qu'à aider les opérateurs à faire face aux vulnérabilités et à les tenir informés des menaces potentielles. Par ailleurs, comme les systèmes de contrôle industriel (SCI) jouent un rôle majeur dans la vulnérabilité des infrastructures critiques, le ministère de la Sécurité publique du Canada organise des symposiums sur les SCI et offre une formation technique sur le sujet. En outre, dans le but d'améliorer la cybersécurité des réseaux d'IIC, le gouvernement fédéral prévoit actuellement mener des exercices pour tester la capacité des opérateurs d'IIC à répondre et à se remettre des attaques potentielles.

Le gouvernement fédéral devrait également adopter un ensemble plus complet de normes sur la cybersécurité des infrastructures critiques qui comprendrait des directives appropriées pour la mise à jour et l'application des dites normes, et ce, en tenant les fournisseurs d'IIC responsables de la sécurité numérique de leurs infrastructures. Ces règlements devraient être neutres sur le plan technologique et reposer sur une approche fondée sur les risques plutôt que sur des mesures prescriptives. Cela leur permettrait de demeurer pertinents malgré l'évolution inévitable de la technologie. Ces règlements ne devraient pas non plus entraver les efforts de collaboration entre les différents acteurs de cybersécurité et d'IIC.

De plus, le Canada devrait renforcer ses efforts de collaboration internationale pour la protection de ses IIC, puisqu'elles peuvent être utilisées comme porte d'entrée pour accéder aux infrastructures d'autres pays, notamment celles des États-Unis. Il est aussi essentiel que le Canada fasse preuve de vigilance en matière de cybersécurité pour maintenir et renforcer les liens de confiance avec ses partenaires économiques.

IMPORTANCE DES RÉSEAUX DE TÉLÉCOMMUNICATIONS

Avec la croissance de l'économie numérique, notre société devient de plus en plus dépendante de la fiabilité des réseaux de télécommunications. Au cours de la crise de la COVID-19, les télécommunications ont été essentielles pour maintenir fonctionnel de nombreux secteurs économiques. Cette dépendance continuera de croître avec le temps, tout comme la nécessité de garantir une protection adéquate des réseaux de télécommunications.

Actuellement, il existe une réglementation limitée concernant la résilience des réseaux de télécommunications aux cyberattaques. Les entreprises de télécommunications ont tout intérêt à créer un réseau hautement fiable, qui favorise une plus grande sécurité de leurs infrastructures. Les décideurs publics restent néanmoins pertinents dans leur capacité à prescrire des mesures de cybersécurité et à veiller à ce que les réseaux canadiens ne prennent pas de retard sur les technologies clés en matière de cybersécurité.

CAS DE LA CORÉE DU SUD
IMPOSER L'APPLICATION DE NORMES NATIONALES DE CYBERSÉCURITÉ AUX INFRASTRUCTURES CRITIQUES

La Corée du Sud a développé ses propres normes de cybersécurité, K-ISMS, et a rendu leur application obligatoire pour les institutions gouvernementales et de nombreuses entreprises du secteur privé ou public telles que les réseaux de télécommunication, les fournisseurs d'accès à Internet, les hôpitaux et les établissements d'enseignement. K-ISMS est un développement de la norme internationale de gestion de la sécurité de l'information ISO 27001, similaire à la norme canadienne ITSG-33. Toutefois, la norme canadienne a été élaborée uniquement pour les ministères et les organismes du gouvernement fédéral.

2.6 DÉFI 4 – S'ADAPTER À L'ÉVOLUTION DE L'ENVIRONNEMENT TECHNOLOGIQUE

2.6.1 Contexte

Les nouvelles technologies, telles que l'IA, l'informatique quantique, les chaines de blocs, la 5G et l'Internet des objets (IdO), présentent chacune des opportunités et des menaces pour la cybersécurité. Bien qu'elles ne soient pas principalement axées sur la sécurité, à l'exception des chaines de blocs, elles ont toutes des implications importantes en matière de cybersécurité et peuvent apporter de nouveaux outils à la fois aux cybercriminels et aux experts de cybersécurité.

› **IA –** La puissance de l'IA est largement reconnue dans de nombreux domaines, mais reste jusqu'à présent marginalement utilisée en cybersécurité. Pour les cybercriminels, l'IA pourrait bonifier les techniques d'attaque actuelles. L'analyse de mégadonnées ou le balayage des réseaux pour identifier des vulnérabilités sont des cas d'utilisation potentiels qui peuvent permettre aux cybercriminels de mieux préparer leurs attaques. Les techniques d'ingénierie sociale ou de piratage peuvent également être améliorées par des outils d'IA qui peuvent imiter le comportement humain, ce qui rend ces tactiques plus difficiles à détecter. D'autre part, l'IA peut améliorer l'efficacité des antivirus et des systèmes de détections des cybermenaces. Elle peut également aider les équipes de cybersécurité en sous-effectif à améliorer leurs capacités de réaction aux attaques.

› **Informatique quantique –** La capacité de l'informatique quantique à casser la plupart des méthodes de cryptage actuelles reste théorique, mais est, selon la plupart des experts, inévitable. Pour garantir que les mesures de protection demeurent efficaces, il est essentiel de mettre en œuvre de nouvelles techniques de cryptage qui ne seront pas vulnérables aux ordinateurs quantiques à venir.

› **Chaines de blocs –** La technologie de chaines de blocs a été développée comme un nouveau moyen de sécuriser des registres en les rendant décentralisés et ainsi impossibles à falsifier. Les chaines de blocs permettent donc d'assurer le suivi exact de transactions. En dehors des cryptomonnaies, cette technologie a actuellement des applications limitées, mais prometteuses dans divers domaines tels que la logistique, les services financiers ou les soins de santé. L'exploitation de tout le potentiel de cette technologie permettrait de sécuriser de nombreux services et réseaux d'information.

Toutefois, son application ne garantit pas toujours une protection absolue. Les réseaux soutenus par les chaines de blocs présentent des vulnérabilités, en particulier à l'interface entre les utilisateurs et le système de chaine de blocs lui-même. Par exemple, le registre cryptographique des Bitcoins n'a jamais été compromis de manière significative depuis sa création, mais les échanges, où les utilisateurs interagissent avec la chaine de blocs, ont été attaqués avec succès à plusieurs reprises.

› **5G –** Les réseaux 5G sont destinés à devenir l'épine dorsale de la future infrastructure numérique, ce qui rend leur cybersécurité très importante pour la société. La 5G s'appuie sur les réseaux 4G à hautes performances qui existeront dans les réseaux pour les années à venir. La 5G améliore les réseaux 4G existants, en permettant la création de multiples nouvelles applications générant des quantités massives de données.

L'évolution des réseaux 4G vers la 5G coïncide avec un changement d'architecture de réseau vers des réseaux virtualisés basés sur des logiciels, avec un potentiel de performances plus élevées, de flexibilité et de latence plus faible pour les applications en temps réel. La nouvelle topologie des réseaux et la virtualisation peuvent entraîner de nouveaux défis en matière de vulnérabilité des réseaux. Cependant, le travail de normalisation diligent effectué par des organisations telles que le 3GPP, le GSMA et le National Institute of Technology (NIST), garantit que les points de contrôle de sécurité modernes utilisent les meilleures pratiques de l'industrie pour surveiller les réseaux de manière efficace et efficiente.

› **Analyse de mégadonnées –** L'utilisation de mégadonnées, rendue possible par l'IdO, l'IA et la 5G, permet à de nombreuses entreprises d'optimiser leurs processus, d'améliorer leurs expériences clients et de mieux comprendre les dynamiques de marché. Malheureusement, les grandes quantités de données générées et stockées par diverses entreprises représentent également des opportunités importantes pour les cybercriminels. Des méthodes d'analyses avancées leur permettent désormais de comparer les données provenant de multiples vols de données et de dresser des profils plus complets de leurs victimes potentielles. D'autre part, les professionnels de la cybersécurité peuvent également utiliser des méthodes d'analyses avancées sur les données d'activité des réseaux pour identifier efficacement les cyberattaques ou les vulnérabilités.

› **Internet des objets (IdO) –** La prolifération des dispositifs IdO dans les milieux résidentiel, commercial et industriel sera favorisée par l'avènement de la 5G qui améliore la capacité et la rapidité des réseaux et réduit leur latence. Allant d'appareils ménagers connectés à des capteurs industriels connectés, le nombre croissant de dispositifs IdO multiplie le nombre de points d'entrée potentiels des cybercriminels dans les réseaux. De nombreux dispositifs IdO (en particulier les applications dédiées au grand public) ne disposent pas d'une protection adéquate, présentent souvent des vulnérabilités connues et sont rarement

mis à jour. En outre, les consommateurs ne sont souvent pas conscients des risques de cybersécurité liés aux dispositifs IdO.

2.6.2 Considérations clés pour les politiques futures

La gestion des risques de cybersécurité résultant de ces nouvelles technologies passe par la recherche et le développement ciblé de nouveaux outils de sécurité et de meilleures pratiques, et par la mise en place d'une main-d'œuvre compétente capable de les mettre en œuvre.

Un soutien financier à la recherche dans chacune de ces technologies existe déjà dans de nombreuses universités canadiennes par le biais de programmes de recherche gouvernementaux. Ces initiatives de recherche sont actuellement soutenues par le Conseil national de recherches du Canada (CNRC), et par le biais de programmes tels que l'Institut canadien de cybersécurité de l'Université du Nouveau-Brunswick et la collaboration CNRC-Waterloo sur l'IA, l'IdO et la cybersécurité de l'Université de Waterloo. Au-delà du financement individuel de chaque programme de recherche, il est également essentiel de promouvoir la collaboration, au niveau national et international.

Pour développer la main-d'œuvre qualifiée nécessaire en cybersécurité, il faut aider les collèges, les universités et les entreprises à attirer les étudiants et les travailleurs des TIC, déjà très convoités, dans le sous-domaine parfois moins attrayant de la cybersécurité. La pénurie de talents dans ce domaine est un problème international causé par la forte demande mondiale dans le secteur technologique. En effet, les emplois dans le domaine de la cybersécurité au Canada sont souvent moins attrayants pour les professionnels des TIC. Pour attirer les talents, le gouvernement fédéral gère déjà un programme d'insertion professionnelle et de financement de stages – le Programme de stages pratiques pour étudiants – qui s'occupe, entre autres, du domaine de la cybersécurité. De plus, le gouvernement soutient les emplois de R&D en cybersécurité dans le secteur privé en finançant directement certaines initiatives de recherche menées par des entreprises par le biais du Programme de coopération en matière de cybersécurité. Néanmoins, la pénurie de talents risque de s'aggraver avec le temps en raison des pressions démographiques. Il est donc important de s'assurer que ces programmes soient efficaces et mis à jour de manière fréquente.

DIVERSITÉ DES PROFILS EN CYBERSÉCURITÉ

La pénurie de main-d'œuvre dans le domaine de la cybersécurité est une préoccupation majeure pour l'industrie et risque de s'aggraver. Pour remédier à ce problème, les entreprises devraient accroître la diversité de leur main-d'œuvre dans le domaine de la cybersécurité. Améliorer de la diversité de genres, d'ethnicités, d'âges, de parcours professionnel et autres est un défi important qui, si relevé, élargira le bassin de talents. Les entreprises devraient également prendre en considération les personnes ayant des formations plus diverses qui ne sont pas nécessairement titulaires de l'habituel diplôme en informatique.

Bien que les fonctions de cybersécurité exigent souvent des compétences techniques, il existe de nombreux postes pour lesquels d'autres formations peuvent être utiles. Par exemple, le manque de sensibilisation à la cybersécurité dans les entreprises, qui constitue un défi majeur pour la cybersécurité (cf. section 2.3), peut être mieux traité par une personne ayant une formation en communication plutôt que par un expert en informatique. Des travailleurs ayant des compétences diverses peuvent trouver de nouvelles solutions pour relever les grands défis de la cybersécurité.

De plus, le recrutement d'individus ayant des parcours académiques et professionnels divers permettrait aux entreprises de combler efficacement d'importantes lacunes. Offrir une formation de base par le biais de stages ou de programmes d'enseignement spécialisés permettrait aux personnes sans diplôme en informatique de remplir plus facilement et plus rapidement certains rôles techniques de base.

CAS DU ROYAUME-UNI
PROGRAMME NATIONAL ENCOURAGEANT LE DÉVELOPPEMENT DE NOUVEAUX TALENTS DANS LE DOMAINE DE LA CYBERSÉCURITÉ

Pour remédier à la pénurie de main-d'œuvre dans le domaine de la cybersécurité, le Royaume-Uni a lancé, en autres, la campagne nationale CyberFirst visant à informer les adolescents de la possibilité d'une carrière dans la cybersécurité et à les encourager à obtenir des diplômes d'enseignement supérieur pertinents au domaine. Cette campagne est orchestrée par le NCSC, l'équivalent britannique du CCC, et soutient les cours de cybersécurité dans les écoles et offre de généreuses bourses d'études et d'apprentissage aux étudiants universitaires qui souhaitent faire carrière dans la cybersécurité.

2.7 DÉFI 5 – RENFORCER LES EFFORTS POLICIERS CONTRE LA CYBERCRIMINALITÉ

2.7.1 Contexte

Les quatre défis précédents se concentrent principalement sur la prévention de la cybercriminalité. Cependant, pour réduire le taux et l'impact des cybercrimes, il est également essentiel d'identifier et de poursuivre les auteurs de ces crimes. Actuellement, les cybercriminels agissent généralement avec une relative impunité – ils se font rarement prendre et encore plus rarement condamner. Cela est dû à trois facteurs principaux: les capacités des criminels qui sont de plus sophistiqués et qui rendent leurs attaques très difficiles à traquer, le manque de capacités des services policiers à faire face au nombre toujours croissant d'attaques, et l'absence de cadre réglementaire international qui complique la coordination des enquêtes sur la cybercriminalité.

- **Capacités des cybercriminels –** Les capacités techniques des cybercriminels vont continuer de s'améliorer, et aucune entité ne peut raisonnablement ralentir cette tendance. La popularisation du réseau Tor (c'est-à-dire le web invisible) permet d'accroître la collaboration et le partage des outils de cybercriminalité tels que les nouveaux logiciels malveillants.
- **Capacités des forces de l'ordre –** On estime souvent que moins de 1% des incidents de cybercriminalité font l'objet d'enquête visant à identifier ou à poursuivre les auteurs. Le taux exact de poursuite des cybercrimes est inconnu, car la plupart d'entre eux ne sont pas signalés. Alors que 20 % des entreprises canadiennes ont déclaré avoir été touchées par des cyberattaques en 2017, seulement 10 % d'entre elles ont signalé ces incidents à la police (Statistique Canada, 2017).

  Le faible taux de poursuite de la cybercriminalité est révélateur des lacunes dans les capacités policières en cybersécurité en termes de ressources humaines, de compétences techniques et de cadre juridique. La mise en place d'une force policière suffisante pour faire face à tous les incidents est irréalisable, mais des ressources supplémentaires sont nécessaires pour investiguer un plus grand nombre d'attaques. Il est encore plus difficile de retrouver les criminels et de produire des preuves admissibles lorsque les ressources et les cadres juridiques font défaut.
- **Cadre réglementaire international –** Établir un cadre réglementaire international de collaboration en matière de cybercriminalité serait idéal, mais demeure impossible à réaliser en pratique. Actuellement, l'accord le plus important est la Convention de Budapest, signée à l'origine par le Conseil de l'Europe en 2001. Par ce traité, 67 pays s'engagent, à partir de 2020, à aligner leurs législations nationales de cybersécurité et à assurer la coopération avec les services policiers des autres nations. Les pays qui s'opposent à la Convention de Budapest soutiennent qu'elle va à l'encontre de leur souveraineté numérique.

De multiples accords bilatéraux et régionaux encadrent également la collaboration entre les pays ayant des points de vue similaires sur la stratégie de lutte contre la cybercriminalité. Par exemple, l'accord États-Unis-Mexique-Canada (ACEUM) comprend des engagements formels pour développer des capacités avancées de réponse aux cyberattaques et pour partager des informations sur la collecte de renseignements et les enquêtes en matière de cybercriminalité.

De multiples forums internationaux favorisent la collaboration entre les pays et les grandes entreprises dans la lutte contre la cybercriminalité. Le Centre pour la cybersécurité du Forum économique mondial et le Forum mondial sur l'expertise en matière de cybercriminalité encouragent tous deux la coopération entre les secteurs public et privé sur de multiples questions liées à la cybercriminalité. D'autres groupes tels que le G7 et INTERPOL ont mis en place des centres de coopération pour la réponse aux cyberattaques qui fournissent des outils permettant de partager rapidement des informations vitales pour les enquêtes.

2.7.2 Considérations clés pour les politiques futures

Le gouvernement du Canada reconnaît dans sa dernière stratégie de cybersécurité la nécessité de ressources supplémentaires pour les efforts policiers en matière de cybercriminalité et a inclus une telle disposition dans son plan d'action 2019. Les services de police, y compris la GRC et d'autres organismes provinciaux et municipaux, ont préconisé l'amélioration de l'infrastructure de collecte de données afin de donner une meilleure image de la situation actuelle en matière de cybercriminalité. Cette connaissance est nécessaire pour s'assurer que les augmentations de ressources prévues sont en adéquation avec l'ampleur de la problématique.

Les plans actuels visant à accroître les capacités de cybersécurité des forces de police s'étendent sur plusieurs années en raison du long processus de recrutement d'experts et/ou de formation des officiers. Compte tenu de la forte croissance de la cybercriminalité, il convient de fixer des objectifs de capacité pour répondre au niveau futur de la cybercriminalité, et non pas au niveau actuel. Des ressources accrues combinées à une méthode plus simple pour signaler les cybercrimes aideraient à avoir une meilleure image de l'état actuel de la cybercriminalité.

Comme la technologie évolue plus vite que les lois, le cadre juridique risque d'être à la traîne en matière de cybercriminalité. Il est toujours utile de le revoir régulièrement pour tenir compte de l'évolution des tactiques des cybercriminels, même si un certain décalage est inévitable. Actuellement, les accusations basées exclusivement sur des preuves digitales sont très rares, ce qui rend l'application des lois de cybercriminalité difficile. Toutefois, en dispensant une formation supplémentaire aux juges et aux jurys sur les tactiques des cybercriminels, on garantirait une meilleure compréhension des preuves présentées au tribunal.

Le développement des capacités policières nationales de cybersécurité n'est qu'une partie de la solution pour poursuivre efficacement les cybercriminels. Les enquêtes et les poursuites dans les affaires internationales nécessitent une application efficace de la loi dans d'autres pays et un cadre de collaboration approprié. À cette fin, le Canada devrait poursuivre ses efforts en faveur d'une plus grande collaboration en matière d'application des lois sur la cybersécurité. En adoptant des initiatives qui favorisent des réponses plus efficaces aux cybercrimes, le Canada peut devenir un leader en matière de cybersécurité et promouvoir de meilleures pratiques législatives auprès de la communauté internationale.

L'ÉCOSYSTÈME DE PROTECTION DES DONNÉES PERSONNELLES

3.1 CONTEXTE MONDIAL

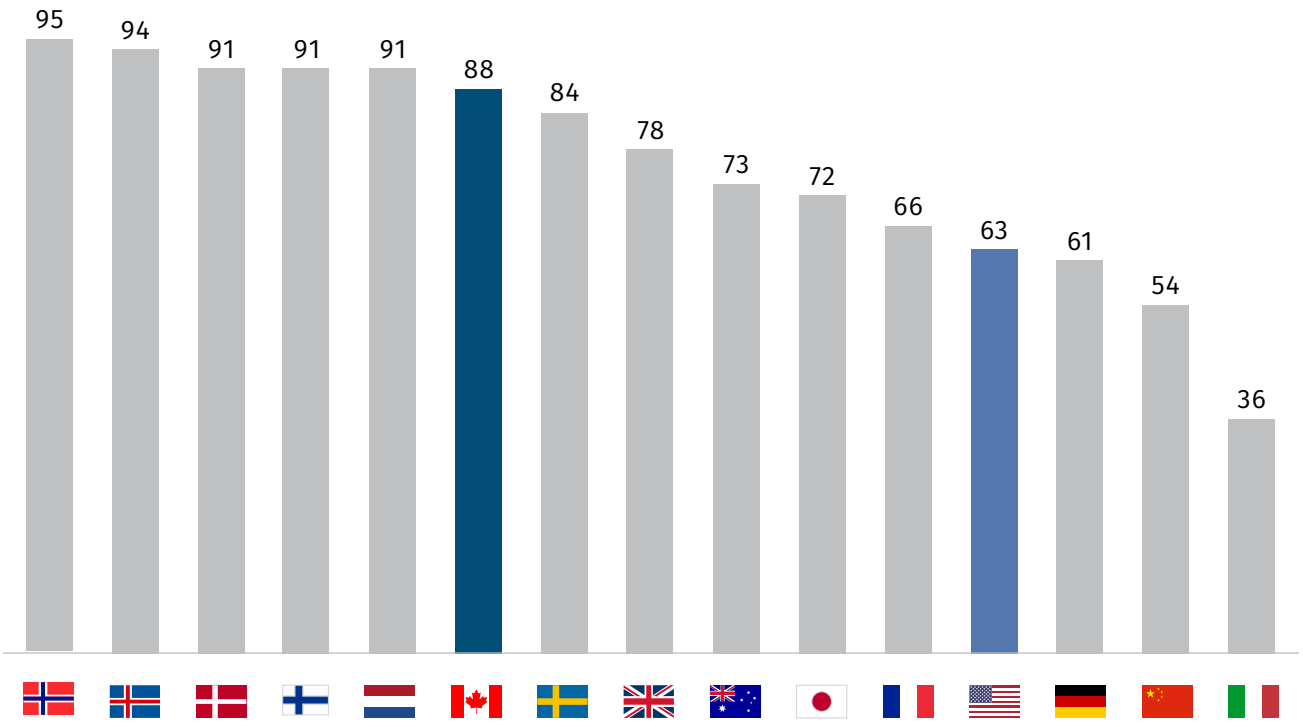
La sensibilisation du public quant à la protection des données personnelles s'est accrue ces dernières, suite à la médiatisation d'importants vols de données et des cas d'abus de collecte de données. La confidentialité est un sujet particulièrement difficile à réglementer dans un environnement commercial et politique en constante évolution, alimenté d'une part par le développement et l'adoption de nouvelles technologies, et d'autre part par des exemples flagrants de mauvaise gestion des données sensibles.

3.1.1 Numérisation accrue du grand public

La population mondiale a déplacé une part croissante de ses activités en ligne, à la recherche d'une flexibilité supplémentaire par rapport aux méthodes traditionnelles. Rien qu'en 2019, le nombre d'internautes dans le monde a augmenté de 7 % pour atteindre 4,5 milliards d'utilisateurs, soit un taux de croissance plus de 6 fois supérieur à celui de la population générale. Au Canada en particulier, le taux de pénétration d'Internet est fixé à 94 %, avec plus de 35 millions d'utilisateurs actifs (DataReportal, 2020).

Les citoyens canadiens sont à l'aise dans l'utilisation de diverses plateformes numériques, comme le montrent le taux d'adoption des services bancaires en ligne, où le Canada n'est dépassé que par quelques pays. Plus des deux tiers (25 millions de personnes) de la population sont également actifs sur les médias sociaux, avec encore près d'un million de nouveaux utilisateurs au cours du second semestre de 2019 (DataReportal, 2020).

Figure 3.1 – Taux d'adoption des services bancaires en ligne par pays [%; 2019; non exhaustif]



Source: Association des banquiers canadiens, Eurostat, Cint, eMarketer, DataReportal, CNNIC, recherche documentaire, Roland Berger

3.1.2 Brèches récentes et cas d'abus de la collecte de données

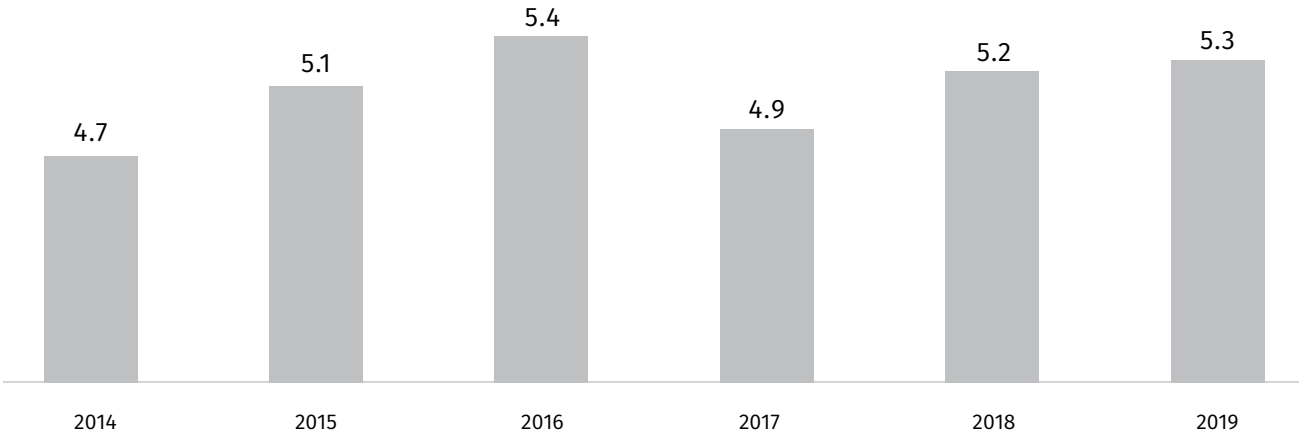
Le niveau croissant de numérisation n'est cependant pas sans risque en termes de confidentialité des données. Deux tendances ont attiré l'attention du grand public: les vols de données dans les grandes organisations et les cas d'abus de collecte de données.

Vol des données

Le coût moyen des vols de données a atteint 5,3 millions de dollars canadiens en 2019 (IBM Security / Ponemon Institute, 2019), un nombre qui n'a cessé de croître au cours des années précédentes. Ce chiffre a été poussé à la hausse par les vols de données importants et largement documentés d'entreprises multinationales, tels que le vol de 3 milliards de comptes d'utilisateurs de Yahoo et la fuite des informations personnelles des clients d'Equifax, qui a exposé les numéros de sécurité sociale et les dates de naissance de 143 millions de personnes (représentant plus de 40 % de la population américaine).

Rien qu'au Canada, des vols récents ont révélé des informations personnelles et sensibles provenant de diverses entités établies, telles qu'Ashley Madison (32 millions de comptes volés par un groupe hacktiviste), Capital One (106 millions de comptes exposés – dont plusieurs canadiens – par un individu aussi lié à 30 autres brèches) et Desjardins (4,2 millions de dossiers exposés par un employé mal intentionné du service informatique).

Figure 3.2 – Coût moyen global des fuites de données [mCAD]



Source: IBM Security / Ponemon Institute, Roland Berger

Cas d'abus de la collecte de données

Certaines grandes entreprises ont également attiré l'attention pour les mauvaises raisons en collectant des informations apparemment inutiles et en faisant craindre un climat de "Big Brother".

Des rapports ayant fait surface dans les dernières années documentent la collecte d'importante quantité de données par de grandes entreprises dont, entre autres exemples, Google (Curran, 2018) (enregistrement détaillé des données de localisation; historique de recherche complet, y compris les recherches supprimées; liste de tout ce qui a été dit à l'assistant Google, y compris les enregistrements audio) et Facebook (Singer, 2018) (suivi des activités des utilisateurs et des non-utilisateurs sur d'autres sites et applications; données faciales biométriques enregistrées sans consentement explicite).

Ces rapports jettent un peu de lumière sur les tactiques commerciales utilisées par les multinationales et alimentent le débat sur la frontière entre les collectes de données appropriées et inappropriées.

3.1.3 Sensibilisation et confiance du grand public

Ces vols de données et ces cas d'abus ont une incidence négative sur la confiance de la population envers les plateformes numériques, et ce, à l'échelle internationale. Au Canada, 76 % des citoyens se disent au moins quelque peu préoccupés par la protection de leur vie privée en ligne, et seulement 40 % estiment que le gouvernement canadien en fait assez pour protéger leurs données (Centre for International Governance Innovation, 2019).

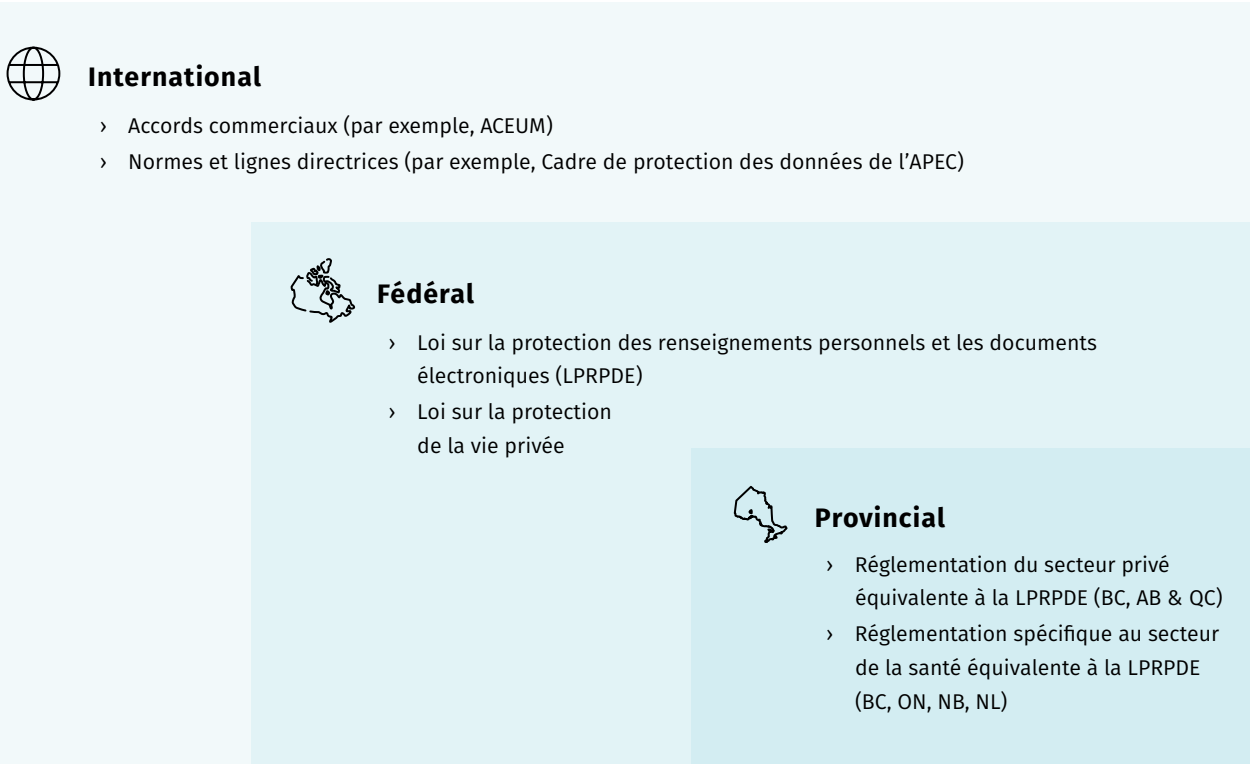
Ces chiffres peuvent sembler inquiétants pour les acteurs de l'économie numérique, qui pourrait craindre un ralentissement de l'adoption des nouvelles technologies en raison des enjeux de confidentialité des données. Ces chiffres peuvent également inquiéter les législateurs, qui ne peuvent pas toujours faire confiance aux grandes entreprises technologiques pour protéger et agir dans l'intérêt de la population. Cela étant dit, l'élément le plus critique pour la croissance de l'économie numérique est le niveau de confiance du grand public. Les décideurs politiques doivent veiller à ce que les consommateurs se sentent protégés pour soutenir l'adoption des technologies numériques.

Bien qu'il n'existe pas de solution parfaite pour régler tous les enjeux liés à la confidentialité des données, il est préférable de disposer d'une orientation et de réglementations claires. Les sections suivantes présentent un aperçu du paysage juridique actuel du Canada, ainsi qu'une incursion dans deux défis majeurs pour les décideurs publics: l'équilibre entre confidentialité et croissance économique, et la complexité des réglementations internationales.

3.2 APERÇU DU CADRE POLITIQUE CANADIEN

Le cadre politique canadien en matière de confidentialité des données s'articule en trois segments: les relations internationales et les accords commerciaux, les politiques fédérales et les politiques provinciales.

Figure 3.3 – Trois champs d'intervention des décideurs publics



Source: Roland Berger

3.2.1 Accords internationaux

Compte tenu de la nature internationale des données numériques et de leurs flux, il reste logique pour les régulateurs de les considérer dans une perspective mondiale. Historiquement, les dispositions relatives aux données dans les accords commerciaux internationaux étaient principalement liées aux efforts de protection de la propriété intellectuelle. Cependant, une nouvelle vague d'accords, mise en évidence par le nouvel accord commercial Canada–États-Unis–Mexique (ACEUM), inclut de plus en plus de dispositions relatives à la protection des données personnelles, intégrant le sujet dans des aspects plus larges du commerce.

L'ACEUM, qui représente une mise à jour significative de l'Accord de libre-échange nord-américain (ALENA), comprend un chapitre sur le digital qui encourage la libre circulation du commerce électronique. Ce chapitre est fondé sur la compréhension commune des parties signataires de la nécessité d'adopter ou de maintenir un cadre juridique protégeant les informations personnelles de tous les utilisateurs du commerce électronique (ACEUM, 2020).

Bien que les détails des cadres juridiques requis soient laissés à la discrétion de chacun des pays, les partenaires sont encouragés à suivre les directives établies par certaines organisations internationales, notamment le forum de coopération économique Asie-Pacifique (APEC[4]) avec son cadre d'action pour la protection des données personnelles (voir l'annexe 1). Les lignes directrices incluses dans ce cadre visent à faciliter l'échange d'informations sans compromettre la protection des informations personnelles.

L'inclusion de règles de protection des données dans l'ACEUM, ainsi que dans d'autres accords internationaux, constitue une étape encourageante vers une collaboration internationale accrue en matière de protection en ligne des intérêts des citoyens et des entreprises et pourrait servir de point de référence pour de futurs accords commerciaux.

3.2.2 Politiques fédérales

Outre la loi sur la protection des renseignements personnels qui régit le droit des individus à accéder aux informations les concernant détenues par les entités fédérales (Commissariat à la protection de la vie privée du Canada, 2019), les obligations légales en matière de confidentialité des données se trouvent dans la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Cette loi, qui repose sur un ensemble de 10 principes (voir figure 3.4), couvre les modalités de stockage des données ainsi que les règles de collecte, d'utilisation et de communication des informations personnelles par les organisations dans le cadre de leurs activités commerciales. L'objectif principal est de trouver un équilibre entre, d'une part, la nécessité pour les organisations d'utiliser les informations personnelles à des fins commerciales légitimes et prévues et, d'autre part, le droit essentiel à la vie privée des personnes (Commissariat à la protection de la vie privée du Canada, 2019).

La LPRPDE s'applique aux entreprises sous réglementation fédérale et aux organisations du secteur privé qui mènent des activités dans la plupart des provinces (à l'exception du Québec, de l'Alberta et de la Colombie-Britannique) ou qui traitent des renseignements personnels qui traversent les frontières provinciales ou nationales. Elle ne s'applique généralement pas aux groupes à but non lucratif et aux organismes de bienfaisance, ni aux partis et associations politiques.

La Loi sur la protection des renseignements personnels numériques, en vigueur depuis 2018, a modifié la LPRPDE pour introduire des obligations de réponse en cas de vols de données, liées à la tenue de registres, au signalement et à la notification (voir figure 3.5). Le non-respect de l'une de ces exigences peut entrainer des sanctions similaires à des infractions criminelles et expose l'organisation et ses administrateurs à des amendes pouvant aller jusqu'à 100 kCAD par violation (Commissariat à la protection de la vie privée du Canada, 2015).

Cette modification de la LPRPDE constitue un élément important pour la protection des données personnelles, en exigeant une responsabilité accrue des organisations et en assurant une plus grande tranquillité d'esprit aux individus, conformément à la tendance mondiale de réglementations similaires. Toutefois, le montant maximum des amendes est bien inférieur à celui d'autres pays, ce qui les rend plus symboliques que dissuasives. À titre de référence, l'amende maximale pour violation du Règlement Général sur la Protection des Données (RGPD) de l'Union européenne peut aller jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise.

4. De l'anglais "Asia-Pacific Economic Cooperation"

Figure 3.4 – Les 10 principes de la LPRPDE

1	**Responsabilité**
2	**Détermination des fins de la collecte d'informations personnelles**
3	**Consentement**
4	**Limitation de la collecte**
5	**Limitation de l'utilisation, de la communication et de la conservation**
6	**Exactitude**
7	**Mesures de sécurité**
8	**Transparence**
9	**Accès aux renseignements personnels**
10	**Possibilité de porter plainte à l'égard du non-respect des principes**

Source : Loi sur la protection des renseignements personnels et les documents électroniques, Roland Berger

Figure 3.5 – Obligations de réponse aux fuites de données introduites dans la LPRPDE

Source : Loi sur la protection des renseignements personnels et les documents électroniques, Roland Berger

3.2.3 Politiques provinciales

De nombreuses provinces ont mis en œuvre des lois supplémentaires sur la protection des données personnelles pour compléter la LPRPDE. La Colombie-Britannique, l'Alberta et le Québec ont adopté des lois qui sont considérées comme suffisamment similaires à la LPRPDE pour leur permettre de réglementer de manière indépendante la protection des données dans le secteur privé.

Certaines provinces (Colombie-Britannique, Ontario, Nouveau-Brunswick et Terre-Neuve-et-Labrador) ont également adopté des lois portant spécifiquement sur le secteur de la santé, qui ont été considérées comme essentiellement similaires à la LPRPDE, et les exemptant ainsi de la surveillance fédérale de la protection de la vie privée dans ce domaine (FairWarning, 2019).

Suite à la récente mise à jour de la LPRPDE qui a introduit des critères d'application plus stricts, certaines provinces envisagent également de revoir leurs propres lois sur la protection des données personnelles. C'est notamment le cas du Québec (à la suite de la fuite de données chez Desjardins) et de l'Ontario (à la suite de multiples vols de données et attaques dans le secteur de la santé).

Le gouvernement du Québec a présenté le projet de loi 64 (Loi modernisant des dispositions législatives en matière de protection des renseignements personnels) en affirmant que les lois actuelles sur la protection des données sont dépassées et ne régissent plus adéquatement l'écosystème numérique en constante évolution. Tout en reproduisant la Loi sur la protection des renseignements personnels numériques en ce qui concerne les exigences de signalement des infractions, la loi augmenterait considérablement les sanctions liées au non-respect de la loi (actuellement fixées à un maximum de 50 kCAD). Les entités du secteur privé pourraient être soumises à des amendes pouvant atteindre le montant le plus élevé entre 25 mCAD ou 4 % de leur chiffre d'affaires mondial, ce qui en ferait la loi sur la protection des renseignements personnels la plus punitive au Canada (Tehrani, Oates, Kappler, & Matziorinis, 2020).

En Ontario, les diverses attaques ayant touché le secteur de la santé ont entrainé l'amendement de la loi sur la protection des renseignements personnels sur la santé (Personal Health Information Protection Act, PHIPA) de la province. Cette nouvelle loi augmente également le montant maximal des sanctions, passant de 500 kCAD à 1 mCAD. En outre, la loi confère de nouveaux pouvoirs au commissaire à la protection de la vie privée de la province, notamment la capacité d'ordonner aux dépositaires d'informations personnelles de santé de cesser de partager ces informations avec des fournisseurs de services électroniques (y compris les entités impliquées dans la communication d'informations personnelles sur la santé par des moyens électroniques, comme les applications mobiles, les portails en ligne et les appareils intelligents). Le renforcement de la protection des informations personnelles de santé par des sanctions accrues et de nouveaux pouvoirs législatifs pourrait cependant ralentir le développement et l'adoption de nouvelles technologies en santé (Morgan, Glover, Scherman, & Chen, 2020).

3.2.4 Principaux défis liés au cadre canadien de protection des données personnelles

Les accords internationaux, les politiques nationales et les réglementations provinciales distinctes visent tous à fournir aux individus des mesures concrètes de protection des renseignements personnels et à défendre leurs intérêts de manière proactive. En ce sens, les décideurs publics sont confrontés à plusieurs défis qui nécessitent la formulation de stratégies claires et efficaces. Les principaux défis peuvent être analysés au travers de deux grands enjeux: la nécessité de trouver un équilibre entre la protection des données personnelles et la croissance de l'économie numérique, et la complexité du paysage législatif international dans un monde se tournant de plus en plus vers le numérique.

3.3 DÉFI 1 – ÉQUILIBRER LA PROTECTION DES DONNÉES PERSONNELLES ET LA CROISSANCE DE L'ÉCONOMIE NUMÉRIQUE

3.3.1 Contexte

L'économie numérique est une industrie propice à l'innovation qui, par conséquent, est en constante évolution. Un tel environnement d'affaires encourage les entreprises à favoriser une mise en marché rapide des nouvelles technologies, et parfois au détriment de la confidentialité et de la sécurité des données.

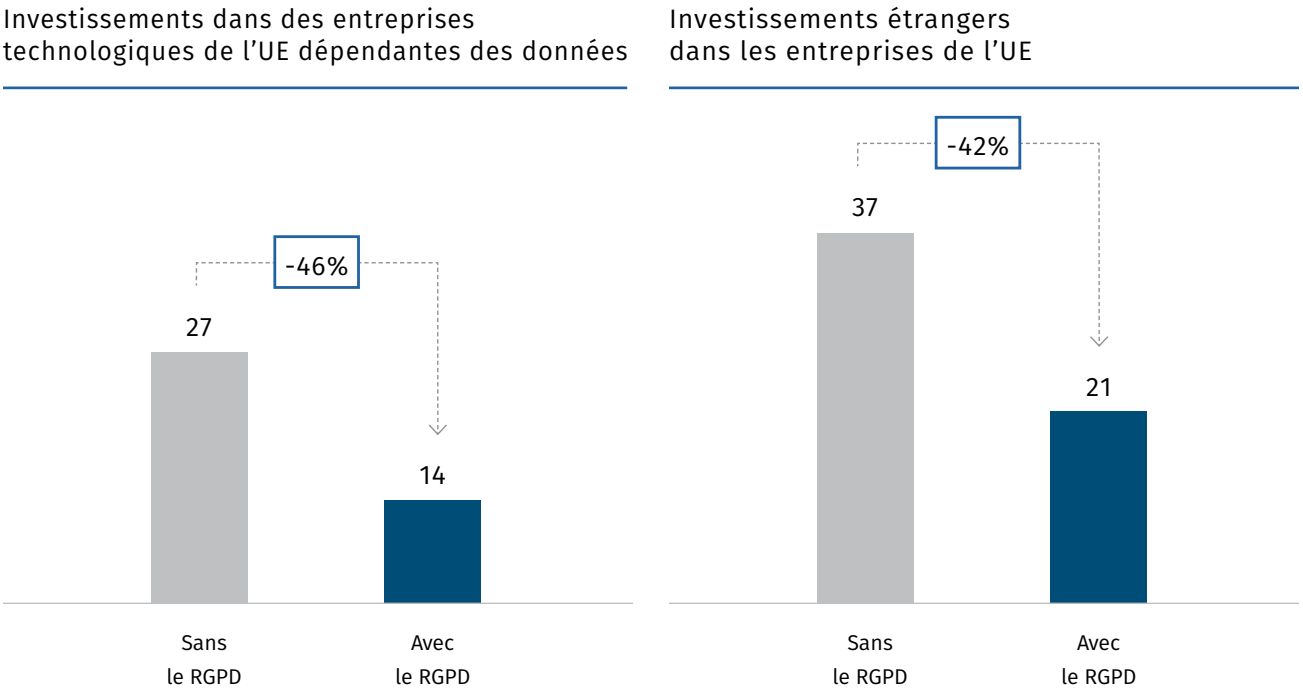
L'équilibre entre la confidentialité des données et l'innovation numérique est primordial à la société actuelle et doit être considéré avec la plus grande attention pour assurer la croissance de l'économie numérique. Bien que les utilisateurs cherchent à profiter des nouvelles technologies, celles-ci ne doivent pas compromettre leur sécurité et leur confidentialité. L'environnement réglementaire devrait chercher à rendre cet équilibre inhérent au déploiement réussi des nouvelles technologies.

La crise actuelle de la COVID-19 offre un excellent exemple de l'équilibre délicat qui doit être trouvé entre la technologie et la confidentialité. Les pays du monde entier ont déployé ou sont en train de déployer des applications de traçage des contacts à la COVID-19 basées sur une variété de technologies et de normes. Le Canada ne fait pas exception, ayant lancé une application à l'échelle nationale en août. Ces applications mobiles sont un formidable exemple d'innovation numérique rapide et pourraient jouer un rôle crucial dans la lutte mondiale contre la COVID-19, en permettant de suivre la propagation du virus et d'informer de manière proactive les individus d'une éventuelle exposition. Toutefois, elle soulève d'importantes questions liées à la confidentialité des données. De nombreux citoyens expriment des inquiétudes quant à l'intensification de la surveillance gouvernementale résultant de la géolocalisation possible avec ces applications (Singer, 2020).

Ces préoccupations en matière de protection de la vie privée ont conduit à une déclaration commune des commissaires à la protection de la vie privée fédéraux, provinciaux et territoriaux, qui ont défini les principes directeurs à respecter. Ils affirment que l'application devrait s'articuler autour des notions de consentement, de transparence et de limitation des objectifs, afin d'aider les Canadiens à prendre la décision éclairée d'utiliser volontairement l'application, sachant qu'elle respecte leur confidentialité (Commissariat à la protection de la vie privée du Canada, 2020).

La frontière entre l'adoption d'une nouvelle technologie numérique et la protection des données personnelles est parfois difficile à tracer. Les États-Unis, d'une part, favorisent généralement l'innovation, ce qui a conduit à de nombreuses avancées technologiques importantes. D'autre part, l'Union européenne a tendance à faire passer le respect de la vie privée en premier. Tout en protégeant fortement les intérêts des individus, cette attention accrue portée à la vie privée semble avoir provoqué une baisse des investissements dans diverses entreprises suite à la mise en œuvre du RGPD, en particulier dans les entreprises européennes dépendantes des données (Jia & Wagman, 2020).

Figure 3.6 – Valeur moyenne des investissements dans les entreprises européennes après la mise en œuvre du RGPD [mCAD]



Source : Jia & Wagman – One-year impact of the GDPR on European Ventures, Roland Berger

3.3.2 Le cas des villes intelligentes

L'utilisation de dispositifs connectés de l'Internet des objets (IdO) pour créer des villes intelligentes offre une multitude de nouvelles possibilités. Ils permettent aux municipalités d'être mieux équipées pour prendre des décisions appuyées sur des données probantes et pour planifier plus efficacement les besoins urbains futurs. Les dispositifs peuvent surveiller, par exemple, le trafic routier, les niveaux de bruit et la pollution atmosphérique, ce qui permet aux villes d'apporter des solutions efficaces et bien ciblées à différents enjeux.

Cependant, plus des données sont collectées, plus les risques d'abus affectant la vie privée des citoyens sont grands. Les objets connectés fournissent également des points d'entrée supplémentaires pour d'éventuelles cyberattaques, qui pourraient entrainer la divulgation des informations personnelles sensibles des citoyens. Des cas récents, tant dans le secteur privé que public, mettent en évidence le besoin émergent de nouvelles réglementations dans ce domaine.

Dans le secteur privé, le projet Sidewalk Labs à Toronto, qui était particulièrement ambitieux, visait à créer un environnement futuriste, où tout pourrait être géré par des dispositifs IdO : des trottoirs chauffants aux auvents rétractables.

La compagnie responsable de ce projet a déclaré que les données collectées auprès des citoyens seraient anonymisées et agrégées (conformément aux principes directeurs définis par les commissaires à la protection de la vie privée), puis mises à la disposition des entreprises et des institutions gouvernementales qui souhaiteraient les utiliser pour des développements futurs. Cependant, l'anonymisation des données n'est pas infaillible et présente un risque de réidentification, accru par la collecte et le stockage des données de localisation. De plus, Sidewalk Labs n'a pas clairement indiqué la manière dont il allait s'assurer du consentement des individus, un droit fondamental couvert par la LPRPDE.

Cette absence de possibilité de "désengagement" à la collecte de données a entrainé une poursuite de la part de l'Association Canadienne des Libertés Civiles (ACLC). Si le consentement est facile à donner lorsqu'une personne installe un assistant intelligent (par exemple, Alexa, Google Home) chez elle, il est beaucoup plus difficile à donner lorsqu'on se déplace à pied dans les rues de Toronto. Citant les mauvaises conditions économiques résultant de la crise COVID-19, Sidewalk Labs a décidé d'abandonner son projet de Toronto (Doctoroff, 2020). Il est clair que les préoccupations du public ont joué un rôle significatif dans cette décision, l'ACLC ayant ciblé les trois niveaux de gouvernement dans son procès.

Dans le secteur public, le Défi des Villes Intelligentes du gouvernement canadien (un concours national encourageant les villes à adopter de nouvelles solutions technologiques) est un exemple où les décideurs publics ont dû trouver un équilibre entre l'innovation et la confidentialité des données. Après son annonce en 2017, tous les commissaires à la protection de la vie privée fédéraux, provinciaux et territoriaux ont adressé une lettre conjointe au ministre de l'Infrastructure et des Collectivités, l'exhortant à prendre des mesures proactives pour veiller à ce que la protection de la vie privée et la sécurité des renseignements personnels soient expressément prises en compte dans la sélection, la conception et la mise en œuvre des propositions gagnantes (Commissariat à la protection de la vie privée du Canada, 2018). Bien que le défi encourage des solutions innovantes aux défis les plus urgents des municipalités, ils craignent que le court délai imparti pour le relever ne relègue la vie privée et la sécurité des données au second plan.

3.3.3 Considérations clés pour les politiques futures

Afin de tenir compte de divers points de vue dans l'élaboration de nouvelles initiatives dans le domaine de la protection des données personnelles, le ministère de l'Innovation, des Sciences et du Développement économique a lancé en 2018 les Consultations nationales sur le numérique et les données, qui visent à recueillir les opinions et les idées des citoyens canadiens. Cela a conduit au lancement de la Charte numérique en 2019 qui décrit un ensemble de 10 principes (voir figure 3.7) visant à accroître la confiance des Canadiens envers les technologies digitales et à mettre l'accent sur l'obligation fiduciaire des dépositaires de données.

La charte cherche à améliorer la protection des données et la perception de sécurité des individus en prescrivant des orientations et des exigences claires pour les entreprises. Toutefois, la Charte n'est pas un document juridique.

Figure 3.7 - Les dix principes de la Charte numérique

1	**Accès universel**
2	**Sûreté et sécurité**
3	**Contrôle et consentement**
4	**Transparence, portabilité et interopérabilité**
5	**Gouvernement numérique ouvert et moderne**
6	**Règles du jeu équitables**
7	**Données numériques pour le bien commun**
8	**Démocratie solide**
9	**Exempt de haine et d'extrémisme violent**
10	**Application rigoureuse et réelle responsabilité**

Source : Charte numérique du Canada, Roland Berger

Pour mettre en œuvre les principes énoncés dans la Charte numérique, le ministre Bains (responsable de la Charte) a annoncé le projet de modernisation de la LPRPDE. Il existe un besoin reconnu de mettre à jour la LPRPDE pour refléter ces principes et renforcer la protection de la vie privée à l'ère numérique (Governement du Canada, 2019).

La proposition de modernisation de la LPRPDE est divisée en 4 sections : accroître le contrôle que peuvent exercer les gens, favoriser l'innovation responsable, améliorer l'application de la loi et la surveillance, et l'évaluation continue. Pour chacun de ces segments, de multiples idées sont exprimées comme moyens de mise en œuvre directe des changements proposés.

La Charte numérique prescrit clairement l'orientation et la stratégie à privilégier au travers de recommandations, mais celles-ci n'ont aucun appui légal. Ce manquement crée une incertitude, voire une confusion, quant à l'approche attendue en matière de gestion des données numériques. Il serait préférable de modifier la loi le plus rapidement possible afin de créer une cohérence entre la réglementation et les lignes directrices décrites dans la Charte numérique. Ce faisant, le Canada minimiserait le risque d'investissement en technologie résultant d'un contexte législatif incertain. De plus, en actualisant la réglementation qui est actuellement considérée par certains comme manquant de mordant (Baer & Newman, 2019), le pays serait mieux placé pour appliquer des normes plus strictes en matière de protection des données personnelles. Il en résulterait un renforcement de la confiance des individus, ce qui favoriserait l'adoption des nouvelles technologies numériques.

Le gouvernement fédéral doit tenir compte des différents règlements adoptés dans le monde (par exemple, la législation américaine, le RGPD de l'Union européenne et les mises à jour discutées au Québec et en Ontario) pour formuler sa nouvelle législation. Le Canada doit adopter une réglementation pertinente dans le contexte mondial, en tenant compte des meilleurs intérêts des Canadiens, notamment en ce qui concerne l'équilibre entre la protection de leurs données et la croissance de l'économie numérique. Compte tenu de l'évolution rapide des technologies, le Canada doit également s'engager à réexaminer fréquemment la législation pour s'assurer qu'elle demeure pertinente.

3.4 DÉFI 2 – NAVIGUER DANS LA COMPLEXITÉ DU PAYSAGE LÉGISLATIF INTERNATIONAL

La confidentialité des données est un concept perçu de manière très différente par des pays partageant des cultures politiques relativement similaires.

Pour l'Union européenne, la protection des données est considérée comme un droit fondamental et est liée aux droits à la dignité des individus. Le droit à la vie privée est inclus dans le système européen des droits fondamentaux, étant apparu comme nécessaire après la Seconde Guerre mondiale. Le langage sous-jacent de la législation européenne en matière de protection des données est centré sur les droits de l'homme et vise à protéger les individus contre le traitement abusif de leurs données personnelles, en définissant comme règle de base que tout traitement de données nécessite une base juridique.

Aux États-Unis, l'approche privilégiée pour la protection des données est liée à l'idéologie de libre marché du pays, qui considère que les individus peuvent utiliser leurs informations personnelles comme une marchandise dans leurs relations commerciales avec des entreprises. La Constitution américaine ne considère pas le droit à la vie privée de la même manière que dans l'Union européenne, ne protégeant les citoyens que contre des types spécifiques de collecte et de traitement des données par le gouvernement, et non par d'autres particuliers (Schwartz & Peifer, 2017).

Cette dichotomie démontre bien la complexité de la gestion de la confidentialité des données à l'échelle mondiale. Cette complexité peut être décomposée en six questions distinctes que les décideurs politiques canadiens doivent prendre en compte lors de l'élaboration de leur politique.

LE POINT DE VUE AMÉRICAIN SUR LA VIE PRIVÉE

En 2011, la Cour suprême a invalidé une loi du Vermont empêchant les pharmacies de vendre des informations d'identification des prescripteurs sans leur consentement explicite. L'arrêt a déclaré que la loi violait la clause de liberté d'expression du premier amendement parce qu'elle limitait l'expression de la commercialisation des produits pharmaceutiques. Cet exemple illustre la conception de la vie privée centrée sur le commerce aux États-Unis. (Schwartz & Peifer, 2017)

3.4.1 Contexte : Enjeux et défis de la protection internationale des données

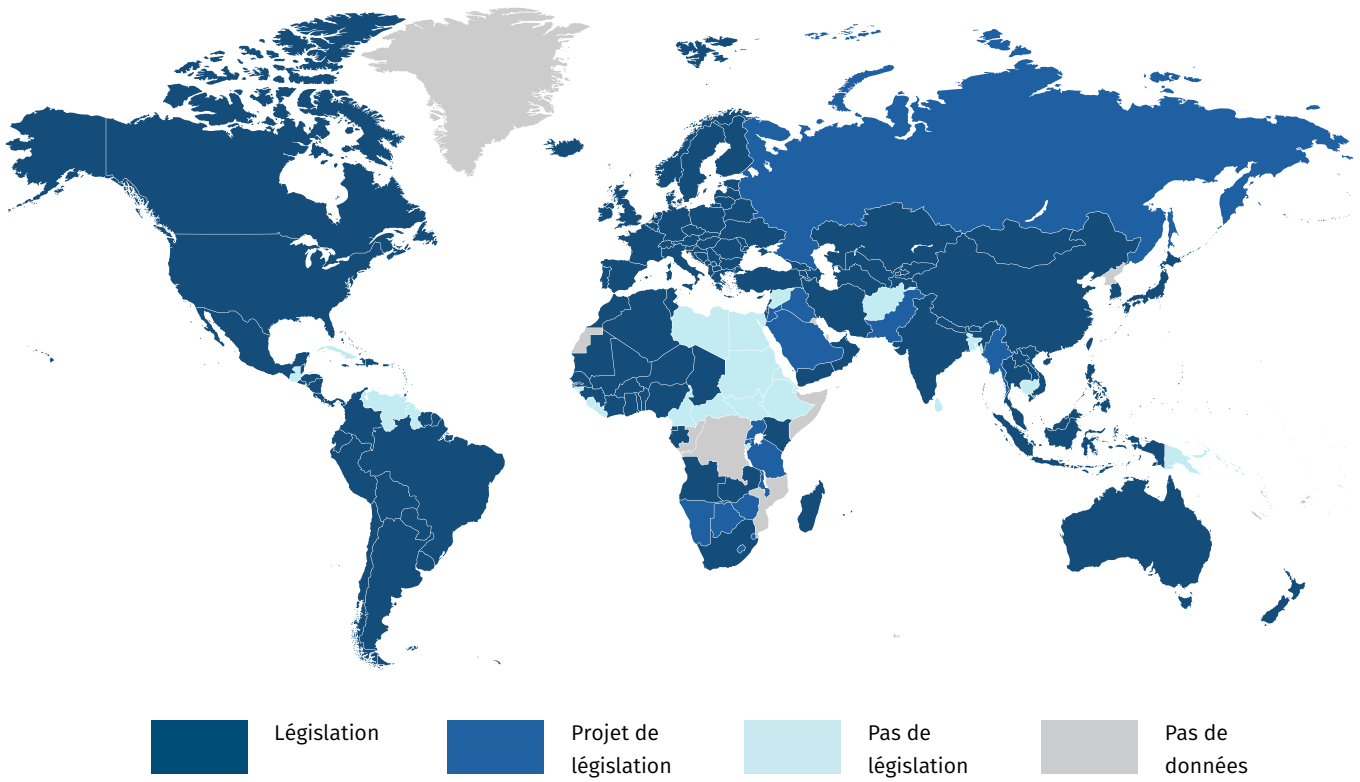
Il existe six enjeux clés interconnectés concernant la protection internationale des données. Chacun d'entre eux présente des défis différents pour les décideurs publics.

3.4.1.1 Variabilité des lois sur la protection des données

La première difficulté associée à la protection internationale des données est la fragmentation et la diversité des lois sur la vie privée dans le monde. La plupart des pays disposent de lois sur la protection des données, mais certaines excluent certains services, comme l'infonuagique, de leur réglementation. D'autres comportent des lacunes et des exemptions, bien que cela soit de moins en moins fréquent. Par exemple, le Japon a supprimé en 2017 une exemption des petites entreprises utilisant des bases de données de moins de 5 000 enregistrements (Hayashi & Yukawa, 2020). Il existe également plusieurs pays, qui ne sont généralement pas de grands partenaires commerciaux du Canada, qui n'ont pas de législation en matière de vie privée, comme le Venezuela et l'Égypte, ou qui sont dans le processus d'adopter leurs premières lois en la matière, comme la Russie et l'Arabie-Saoudite.

Le réseau des lois sur la protection des données personnelles est complexe en raison des nombreux accords commerciaux qui exigent une adéquation entre les différentes normes pour garantir la libre circulation des informations. Si les dispositions ne sont pas symétriques, les pays peuvent conclure des accords collatéraux spécifiques, tels que le Bouclier de protection des données entre l'Union européenne et les États-Unis. En s'engageant dans de tels cadres réglementaires distincts, la nécessité de créer un ensemble commun de lignes directrices internationales est limitée, ce qui pourrait à terme diminuer la collaboration économique internationale.

Figure 3.8 – Présence de législations relatives à la protection des données et de la vie privée dans le monde [2020]



Source : CNUCED, Roland Berger

3.4.1.2 Émergence de nouvelles technologies

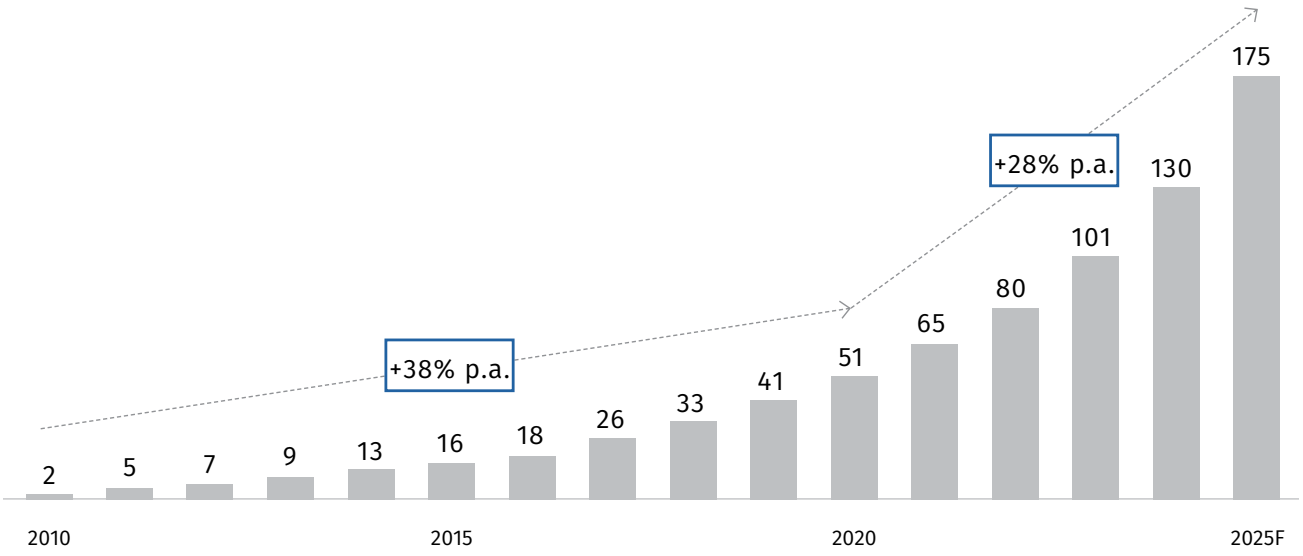
Les nouvelles technologies offrent des possibilités révolutionnaires pour l'économie numérique, mais posent également un défi important aux responsables politiques et aux législateurs qui s'efforcent de mettre en œuvre des réglementations pertinentes dans un environnement en évolution constante. Les risques de violation de la sécurité et de mauvaise gestion de la vie privée augmentent en raison de l'émergence des nouvelles technologies. De nombreuses technologies spécifiques soulèvent des questions en matière de confidentialité des données, en particulier l'infonuagique, l'Internet des objets et l'analyse des mégadonnées.

Infonuagique – L'infonuagique soulève plusieurs questions complexes liées aux transferts transfrontaliers de données. En connectant les utilisateurs à l'échelle mondiale, les fournisseurs de services d'infonuagique peuvent théoriquement stocker des données à l'étranger et les communiquer aux clients en utilisant les infrastructures locales. Pour limiter l'exposition potentielle des données des citoyens, certains pays ont mis en place des règles de localisation des données imposant aux fournisseurs de services étrangers de stocker les données sur leur territoire. Il n'y a pas d'accord unanime sur les moyens de réglementer l'infonuagique, et certains pays (dont le Canada) favorisent plutôt la libre circulation de l'information dans leurs accords commerciaux internationaux (ACEUM, 2020).

Internet des objets (IdO) – Le nombre d'appareils connectés et la quantité de données qu'ils génèrent augmentent rapidement, ce qui engendre plus d'échanges d'informations par-delà les frontières internationales. Les cyberattaques sur l'IdO sont de plus en plus fréquentes, ce qui souligne la nécessité d'une coopération et d'une réglementation internationales. Par exemple, 80 % des responsables de cybersécurité en santé en Chine, en Allemagne, au Japon, au Royaume-Uni et aux États-Unis ont signalé des attaques sur leurs dispositifs connectés entre 2018 et 2019 (Irdeto, 2019).

Analyse des mégadonnées – Les grandes bases de données sont de plus en plus ciblées par les pirates informatiques étant donné la quantité d'informations disponibles. La grande quantité de données recueillies auprès d'utilisateurs du monde entier est très utile aux organisations qui cherchent à mieux comprendre les dynamiques du marché et à préparer leurs futurs projets. Cependant, le principe sous-jacent des mégadonnées, qui consiste à collecter toutes les données, et pas seulement celles qui sont directement pertinentes, est en opposition avec les principes de limitation de la collecte de données au niveau mondial (tels que décrits dans le cadre de protection des données personnelles de l'APEC). Ces principes, des lignes directrices plutôt qu'une réglementation contraignante, offrent une marge de manœuvre aux entreprises, ce qui peut avoir un effet négatif sur la confidentialité des individus.

Figure 3.9 – Volume mondial de données créées par année [zettabytes]



Source : Centre d'études stratégiques et internationales, Roland Berger

3.4.1.3 Transferts transfrontaliers de données

Les législations sur les transferts transfrontaliers de données sont utiles pour comprendre la position des pays sur la confidentialité des données et la circulation des informations. Certains pays, comme les États-Unis, ont peu de restrictions sur le transfert de données personnelles vers des juridictions étrangères (Congressional Research Service, 2019). Les autres pays autres préfèrent recourir à des exemptions basées sur des “circonstances exceptionnelles” ou des “exceptions existantes”.

Des droits de transferts transfrontaliers de données basées sur des **circonstances exceptionnelles** sont inclus dans de nombreuses lois sur la protection des données personnelles et permettent d’autoriser les transferts transfrontaliers dans des cas spécifiques (Centre for Information Policy Leadership, 2015). Ces transferts peuvent être autorisés, entre autres, lorsque les données sont nécessaires à l’exécution d’un contrat, ou lorsqu’elles sont utilisées dans le cadre d’une procédure judiciaire ou pour exercer des droits légaux.

Les **exceptions existantes** sont moins homogènes, mais suivent généralement une combinaison de quatre approches, qui présentent chacune des forces et des faiblesses différentes.

- L’approche par **suffisance**, qui équivaut au maintien d’une liste blanche, repose sur l’évaluation des juridictions étrangères, pour s’assurer qu’elles offrent un niveau de protection suffisant. Cette approche favorise l’interopérabilité entre certains pays, mais peut causer des préjudices aux pays jugés inadéquats. En se basant sur cette évaluation, des accords commerciaux entre les pays jugés adéquats peuvent comprendre des dispositions visant à encourager la libre circulation des informations, comme c’est le cas pour l’ACEUM.
- L’approche par **règles contraignantes** permet d’évaluer si une entreprise spécifique a mis en place des processus et des mécanismes (comme un processus d’examen indépendant) offrant un niveau de protection approprié des données personnelles. Elle permet la libre circulation de l’information entre les entreprises participantes et encourage la mise en œuvre des meilleures pratiques, mais constitue un exercice exigeant qui n’est pas facilement transférable à d’autres groupes.
- L’approche par **contrats types** consiste à examiner les contrats pour déterminer si un libellé spécifique apparaît afin d’offrir une protection suffisante. Cette approche favorise l’interopérabilité avec d’autres groupes, mais certains partenaires peuvent contourner la disposition sur une technicalité.
- Enfin, l’approche par **consentement** détermine si les individus peuvent consentir au transfert de leurs données personnelles. C’est effectivement l’approche la plus claire, présentant la charge de conformité la plus faible pour les organisations, mais elle peut exposer les entreprises à des plaintes et à des litiges concernant des interprétations divergentes.

La plupart des pays combinent plusieurs approches afin d’établir des mécanismes de transferts transfrontaliers, car aucune approche unique ne convient à tous les cas. Il n’existe pas non plus de combinaison standard, ce qui oblige les pays à négocier des accords individuels et limite l’interopérabilité des combinaisons choisies.

3.4.1.4 Équilibre entre surveillance et protection des données personnelles

Cet enjeu constitue une question éthique qui limite les accords internationaux sur la protection de la vie privée. Les pays considèrent que la protection des données est, au moins à un certain niveau, un droit indéniable des citoyens. Toutefois, une surveillance généralisée est souvent autorisée dans le cadre de préoccupations de sécurité nationale.

De nombreuses lois nationales dans le monde prévoient des exceptions pour des raisons de sécurité nationale. Le Patriot Act des États-Unis permet notamment au gouvernement de surveiller les communications téléphoniques et électroniques et de suivre l’activité Internet des Américains, qu’ils soient sur le territoire national ou international. Bien qu’il vise le terrorisme, il a été constaté en 2015 qu’au cours des 14 années où il a été utilisé, aucun cas de terrorisme majeur n’a été résolu grâce à la surveillance qu’il a autorisée (Ybarra, 2015). Cette révélation soulève des questions sur l’équilibre délicat entre les techniques de surveillance appropriées ou excessives.

Les gouvernements du monde entier adoptent des positions différentes sur cet enjeu, ce qui est une source importante de frictions.

3.4.1.5 Renforcement des sanctions en matière de protection des données et de leur application par les partenaires commerciaux

Les organisations jugées responsables de fuites de données ont récemment été soumises à des amendes et des sanctions de plus en plus sévères. De nombreuses grandes organisations de renom ont subi des fuites qui ont eu des conséquences sans précédent, bien plus importantes que celles prévues dans les réglementations existantes. Les États-Unis sont considérés comme un leader en termes d'imposition de sanctions pour des fuites, ayant imposé des amendes massives ces dernières années. D'autres pays ont également prévu ou ont déjà modifié leurs lois sur la protection des données personnelles afin de renforcer leurs pouvoirs, comme, par exemple, l'Union européenne (RGPD, 2016) et l'Australie (Office of the Australian Information Commissioner, 2018).

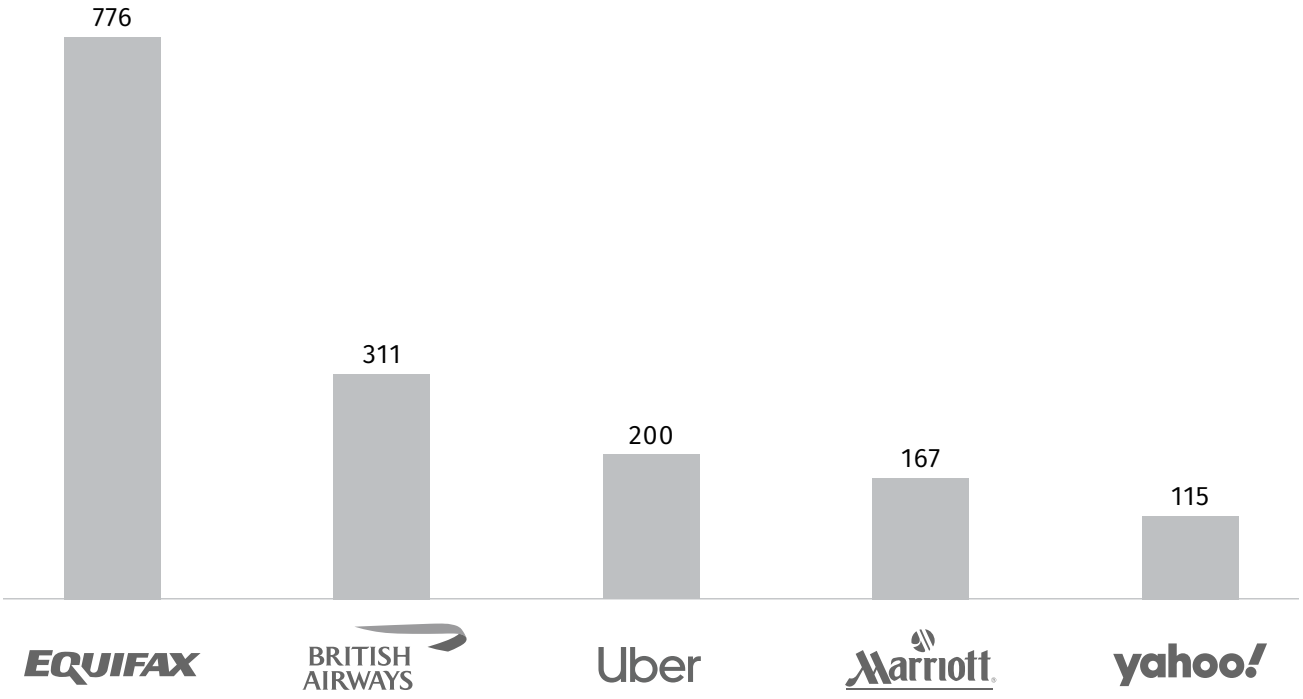
Ces sanctions accrues s'adressent à toutes les parties concernées par une fuite de données :

- **L'entreprise ciblée –** De lourdes amendes et sanctions envoient un message clair concernant la réforme nécessaire des pratiques internes;
- **Les individus concernés –** Les amendes constituent une forme nécessaire de réparation du préjudice subi du fait d'une infraction;
- **L'industrie au sens large –** Les sanctions agissent comme une onde de choc parmi les entreprises similaires, qui pourraient être plus enclines à adopter les meilleures pratiques plutôt que de se voir imposer des amendes similaires.

Ces amendes contribuent à faire comprendre à toutes les parties que la protection des données est importante, mais elles manquent d'uniformité. Le Canada est à la traîne des États-Unis et de l'Europe avec des amendes allant jusqu'à 100 kCAD seulement, ce qui représente une simple amende symbolique pour les grandes multinationales.

36

Figure 3.10 – Les cinq plus importantes pénalités imposées en raison d'une fuite de données [mCAD ; en date de juillet 2020]



Source : OSC, Roland Berger

3.4.1.6 Identification de la juridiction liée à une infraction aux lois sur la protection des données personnelles

L'identification de la juridiction liée à une infraction, une composante majeure du droit, est rendue de plus en plus difficile à établir en matière de protection des données, en raison de la nature internationale des flux de données. La traçabilité des données et l'absence d'un accord mondial sur la protection des données sont des facteurs qui rendent plus complexe l'identification de la juridiction pour l'application des réglementations.

La plupart des législations nationales visent à réglementer toutes les activités visant ses citoyens, quel que soit le lieu d'incorporation de l'entreprise coupable. Le RGPD est l'exemple le plus complet d'une telle réglementation, qui s'applique à toute organisation offrant des biens et des services aux citoyens européens ou surveillant leur comportement.

Certains pays ont adopté des réglementations pour des secteurs spécifiques. Par exemple, le Child Online Privacy Protection Act (COPPA) américain s'étend aux prestataires de services étrangers qui dirigent leurs activités vers les enfants américains ou qui recueillent des informations auprès d'eux (Federal Trade Commission, 2000).

Cependant, l'adoption de lois et de politiques internationales exigera un alignement plus fort entre les pays, un objectif qui est très difficile à atteindre. Le RGPD est un rare exemple de coopération réussie, car il mobilise un large consortium de pays autour de cette question cruciale.

3.4.2 Considérations clés pour les politiques futures

L'analyse de ces six enjeux expose la complexité de la réglementation internationale en matière de protection des données personnelles. La définition culturelle de la vie privée, la disparité des opinions et l'évolution de l'environnement technologique sont des difficultés importantes pour tout pays tentant de faire avancer leur idéologie et leurs réglementations dans l'espoir d'établir une norme internationale.

Les décideurs publics canadiens doivent tenir compte de chacun de ces enjeux, en gardant à l'esprit une perspective nationale et internationale, lorsqu'ils conçoivent et mettent en œuvre des politiques de protection des données personnelles. Il n'y a pas de solutions parfaites concernant la protection des données. Il y a cependant des choix à faire en ce qui concerne les orientations à prendre et les futurs règlements à adopter.

Les nouvelles technologies doivent-elles être adoptées immédiatement pour encourager la croissance économique et l'innovation technologique, ou faut-il se concentrer sur un contrôle et une réglementation accrue, au risque de prendre du retard par rapport aux autres pays?

Le Canada devrait-il établir ses propres exigences en matière de transferts transfrontaliers de données personnelles, ou devrait-il suivre des exigences strictes mises en œuvre par des réglementations telles que le RGPD?

Les dispositions relatives à la surveillance dans le cadre de la sécurité nationale doivent-elles être plus détaillées et restreintes, ou doivent-elles être assouplies pour permettre de déjouer le plus grand nombre de complots terroristes possibles?

Chacune de ces positions présente des avantages valables, mais aussi des inconvénients. Ces décisions devraient être prises de manière cohérente avec la politique étrangère du Canada et tenir compte de l'évolution de l'environnement technologique et législatif. Les décideurs publics devraient poursuivre leurs efforts actuels pour inclure dans les accords commerciaux des dispositions relatives aux nouvelles technologies et aux transferts transfrontaliers de données. D'autres principes devraient également guider l'action des décideurs publics, dont la révision des montants des pénalités liées aux fuites de données en se rapprochant des positions adoptées par les États-Unis ou l'UE ainsi que l'adoption d'une disposition permettant de poursuivre les entités étrangères dont les activités concernent des citoyens canadiens.

Les politiques de protection des données personnelles doivent être fréquemment révisées pour s'assurer qu'elles restent en phase avec l'évolution des technologies, des priorités nationales et des relations internationales. Pour le Canada, adopter une position de leader d'opinion en matière de protection des données est une bonne stratégie pour cet enjeu sensible et peut contribuer à favoriser une collaboration internationale conforme à la perception qu'a le Canada sur la question.

REMARQUES FINALES

L'évolution des technologies numériques constitue un défi important pour les décideurs publics du monde entier. Les cyberattaques, qui menacent tout, de l'intégrité des informations personnelles à la résilience des infrastructures critiques, ont augmenté ces dernières années et ne montrent aucun signe de ralentissement. La nature dématérialisée et de plus en plus mondiale des données exige une attention accrue de la part des décideurs publics, tant au niveau local qu'international.

La cybersécurité et la protection des données personnelles sont des sujets à grande portée qui ont des implications éthiques, juridiques, sociétales et commerciales. Les principaux enjeux rencontrés par les régulateurs peuvent être résumés par les sept défis décrits dans ce document :

1. Améliorer la littéracie numérique du grand public – En sensibilisant les individus et les organisations aux menaces que représentent les cyberattaques, les décideurs publics contribueront à consolider la première ligne de défense contre les menaces futures;
2. Soutenir les institutions plus petites dans leur transformation numérique – En fournissant des outils et des ressources supplémentaires aux petites institutions qui ne disposent pas des compétences nécessaires pour protéger correctement les données qu'elles gèrent, les décideurs publics contribueront à la croissance continue et sûre de l'économie numérique;
3. Sécuriser les infrastructures critiques et les réseaux gouvernementaux – En renforçant les normes et la responsabilité des fournisseurs d'infrastructures critiques et en leur offrant les lignes directrices nécessaires, les décideurs publics réduiront le risque de perturbation;
4. S'adapter à l'évolution de l'environnement technologique – Préparer la main-d'œuvre de demain et encourager la recherche et le développement dans des domaines clés est essentiel pour les efforts futurs dans la lutte contre les cyberattaques;
5. Renforcer les efforts policiers contre la cybercriminalité – En assurant des ressources suffisantes et en améliorant les capacités des forces policières et du système juridique, le pays disposera de meilleurs moyens pour condamner les cybercriminels;
6. Équilibrer la protection des données personnelles et la croissance de l'économie numérique – En introduisant des principes tels que ceux énoncés par la Charte numérique dans un texte législatif actualisé, les décideurs politiques canadiens veilleront à ce que l'innovation numérique se fasse dans le respect de la confidentialité des données;
7. Naviguer dans la complexité du paysage législatif international - En formulant sa stratégie sur la protection internationale des données, l'émergence des technologies, les transferts de données transfrontaliers, la surveillance et le renforcement de l'application des lois, le Canada agira comme un leader d'opinion et encouragera la collaboration internationale.

En relevant ces défis tout en respectant ses valeurs fondamentales, le Canada sera en mesure de mieux protéger ses citoyens, ses entreprises, ses infrastructures essentielles et ses institutions gouvernementales, ainsi que d'encourager la collaboration internationale en matière de cybersécurité et de confidentialité des données.

ANNEXE

Créé en 2005 et révisé en 2015, le cadre de protection des données personnelles de la Coopération économique Asie-Pacifique (APEC) réaffirme la valeur de la vie privée dans le contexte de la promotion du commerce électronique dans toute la région Asie-Pacifique. Le cadre élaboré par ce forum, dont le Canada est l'une des douze nations fondatrices, identifie neuf principes à la base des pratiques éthiques en matière d'information :

- **Prévention des préjudices :** la protection des données personnelles doit être conçue pour empêcher l'utilisation abusive de ces informations, et les mesures correctives doivent être proportionnelles à la probabilité et à la gravité des préjudices possibles par la collecte, l'utilisation et le transfert d'informations;
- **Préavis :** les responsables du traitement des informations personnelles doivent fournir des déclarations claires sur leurs pratiques, notamment sur le fait que des informations personnelles sont collectées, l'objectif de la collecte, les types d'organisations auxquelles les informations peuvent être divulguées et les choix offerts pour limiter l'utilisation et la divulgation des informations personnelles;
- **Limitation de la collecte :** la collecte d'informations personnelles doit être limitée aux informations qui sont pertinentes pour les objectifs de la collecte;
- **Utilisation des informations personnelles :** les informations personnelles collectées ne doivent être utilisées que pour atteindre les objectifs de la collecte, sauf avec le consentement de la personne dont les informations sont collectées, lorsque cela est nécessaire pour fournir un service demandé par la personne ou par l'autorité de la loi et d'autres instruments juridiques;
- **Liberté de choix :** le cas échéant, les personnes devraient disposer de mécanismes clairs, accessibles et abordables pour exercer un choix en matière de collecte, d'utilisation et de divulgation de leurs informations personnelles;
- **Intégrité des informations personnelles :** les informations personnelles doivent être exactes, complètes et mises à jour dans la mesure nécessaire aux fins de leur utilisation;
- **Mesures de sécurité :** les informations personnelles doivent être protégées par des mesures de sécurité appropriées. Ces garanties doivent être proportionnelles à la probabilité et à la gravité du préjudice possible et à la sensibilité des informations;
- **Accès et correction :** les individus devraient pouvoir:
  - obtenir la confirmation que le responsable du traitement des données personnelles détient des informations personnelles les concernant;
  - demander les informations personnelles recueillies les concernant;
  - contester l'exactitude de leurs informations personnelles et de faire rectifier ou supprimer ces informations.
- **Responsabilité :** les entités traitant des données personnelles doivent être responsable du respect des mesures qui donnent effet aux principes énoncés ci-dessus.

RÉFÉRENCES

- ACEUM. (2020). *United States-Mexico-Canada Agreement Digital Trade Chapter.*
- Association des banquiers canadiens. (2019, Mars 13). *Fiche info - Les Canadiens et leurs activité bancaires.* Récupéré sur Association des banquiers canadiens: https://cba.ca/technology-and-banking
- Baer, A., & Newman, S. (2019, June 26). *Canada's New Digital Charter and What This Means For PIPEDA.* Récupéré sur Mondaq: https://www.mondaq.com/canada/privacy-protection/818948/canada39s-new-digital-charter-and-what-this-means-for-pipeda
- Britneff, B. (2020, June 18). *Coronavirus contact-tracing app to launch nationally in early July, Trudeau says.* Récupéré sur Global News: https://globalnews.ca/news/7079851/coronavirus-tracing-app-launch-nationally/
- Center for Strategic and International Studies. (2018). *Economic Impact of Cybercrime - No Slowing Down. McAfee.*
- Centre for Information Policy Leadership. (2015). *Cross-Border Data Transfer Mechanisms.*
- Centre for International Governance Innovation. (2019). *Internet Security & Trust.*
- CNUCED. (2016). *Data protection regulations and international data flows: Implications for trade and development.* New York and Geneva: United Nations Publication.
- CNUCED. (2020, February 4). *Data Protection and Privacy Legislation Worldwide.* Récupéré sur United Nations Conference on Trade and Development: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
- Commissariat à la protection de la vie privée du Canada. (2015). *Loi sur la protection des renseignements personnels numériques.*
- Commissariat à la protection de la vie privée du Canada. (2018). *Lettre conjointe au Ministre de l'Infrastructure et des Collectivités au sujet du défi des villes intelligentes.*
- Commissariat à la protection de la vie privée du Canada. (2018, Avril 26). *Selon les gardiens du droit à la vie privée, les initiatives sur les villes intelligentes doivent prévoir des mesures de protection de la vie privée.* Récupéré sur Commissariat à la protection de la vie privée du Canada: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_180426/
- Commissariat à la protection de la vie privée du Canada. (2019). *Loi sur la protection des renseignements personnels.*
- Commissariat à la protection de la vie privée du Canada. (2019). *Loi sur la protection des renseignements personnels et les documents électroniques.*
- Commissariat à la protection de la vie privée du Canada. (2020, Mai 7). *Appuyer la santé publique et bâtir la confiance des Canadiens : principes de protection de la vie privée et des renseignements personnels pour les applications de traçage des contacts et autres applications similaires.* Récupéré sur Commissariat à la protection de la vie privée du Canada: https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/
- Congressional Research Service. (2019). *Data Flows, Online Privacy, and Trade Policy.*
- Curran, D. (2018). Are you ready? Here is all the data Facebook and Google have on you. *The Guardian.*
- Dalberg / Intel. (2016). Decoding diversity: the financial and economic returns of diversity in tech.
- DataReportal. (2020). *Digital 2020: Canada.*
- Doctoroff, D. L. (2020, May 7). *Why we're no longer pursuing the Quayside project – and what's next for Sidewalk Labs.* Récupéré sur Medium: https://medium.com/sidewalk-talk/why-were-no-longer-pursuing-the-quayside-project-and-what-s-next-for-sidewalk-labs-9a61de3fee3a
- Electronic Privacy Information Center. (Multiple years). *Investigations of Google Street View.* Récupéré sur EPIC.org: https://epic.org/privacy/streetview/
- European Commission. (2018). Women in the Digital Age.
- Eurostat. (2020). *Individuals using the Internet for Internet banking.*

- FairWarning. (2019, March 20). *Canadian Data Privacy Laws, Security Frameworks, and Cloud Compliance.* Récupéré sur FairWarning: https://www.fairwarning.com/insights/blog/canadian-data-privacy-laws-security-frameworks-and-cloud-compliance
- Federal Trade Commission. (2000). *COPPA.*
- Forum de coopération économique Asie-Pacifique. (2015). *Asia-Pacific Economic Cooperation Privacy Framework.*
- Fraser, D., & Dykema, S. (2018, August 6). *The Digital Privacy Act: 5 FAQs about the new mandatory breach response obligations effective November 1, 2018.* Récupéré sur Mondaq: https://www.mondaq.com/canada/privacy-protection/725602/the-digital-privacy-act-5-faqs-about-the-new-mandatory-breach-response-obligations-effective-november-1-2018
- Gemalto. (2018). *Breach Level Index.*
- Governement du Canada. (2019). *Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques.*
- Hayashi, H., & Yukawa, M. (2020). *Japan: Data Protection Laws and Regulations 2020.*
- IBM Security / Ponemon Institute. (2019). *Cost of a Data Breach Report.*
- Innovation, Sciences et Developpement économique Canada. (2019). *La Charte numérique du Canada en action: un plan par des Canadiens, pour les Canadiens.*
- Irdeto. (2019). *Irdeto Global Connected Industries Cybersecurity Survey: IoT cyberattacks are the norm, the security mindset isn't.*
- Jia, J., & Wagman, L. (2020). *The One-Year Impact of the General Data Protection Regulation (GDPR) on European Ventures.*
- Morgan, C., Glover, D., Scherman, M., & Chen, E. Y. (2020, June 24). *Amendments to Ontario's health information legislation bring new obligations and penalties.* Récupéré sur Mondaq: https://www.mondaq.com/canada/privacy-protection/957346/amendments-to-ontario39s-health-information-legislation-bring-new-obligations-and-penalties
- Office of the Australian Information Commissioner. (2018, April 9). *OAIC Guide to Privacy Regulatory Action.* Récupéré sur McCullough Robertson: https://www.mccullough.com.au/2019/04/09/its-no-secret-10-million-penalties-to-be-introduced-for-privacy-law-breaches/
- Pearson, J. (2019, April 17). *Canada is Getting Sued Over Sidewalk Labs' 'Smart City' In Toronto.* Récupéré sur Vice News: https://www.vice.com/en_us/article/gy4bgj/canada-is-getting-sued-over-sidewalk-labs-smart-city-in-toronto
- RGPD. (2016). *Réglement général sur la protection des données.* Récupéré sur General Data Protection Regulation.
- Rotenberg, M. (2016). *Promoting innovation, protecting privacy.* Récupéré sur OECD Observer: https://oecdobserver.org/news/fullstory.php/aid/5593/Promoting_innovation,_protecting_privacy.html
- Schwartz, P. M., & Peifer, K.-N. (2017, November 7). Transatlantic Data Privacy. *Georgetown Law Journal,* pp. 115-179.
- Singer, N. (2018). What you don't know about how Facebook uses your data. *The New York Times.*
- Singer, N. (2020, July 8). *Virus-tracing apps are rife with problems. Governments are rushing to fix them.* Récupéré sur The New York Times: https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html
- Statistique Canada. (2017). Profil des entreprises canadiennes qui signalent les cybercrimes à la police.
- Statistique Canada. (2019). Les cybercrimes déclarés par la police au Canada.
- Statistique Canada. (2019). Table: 14-10-0068-01.
- Tehrani, M., Oates, C., Kappler, J., & Matziorinis, P. (2020, June 24). *Quebec to introduce the most punitive privacy laws in Canada - with fines of up to $25 million.* Récupéré sur Mondaq: https://www.mondaq.com/canada/privacy-protection/956848/quebec-to-introduce-the-most-punitive-privacy-laws-in-canada--with-fines-of-up-to-25-million
- Verizon. (2020). *Data Breach Investigations Report.*
- Ybarra, M. (2015). FBI admits no major cases cracked with Patriot Act snooping powers. *The Washington Times.*


HUAWEI
Roland
Berger

AVIS DE RECOURS EN RÉVISION

RÉVISION

a) Pouvoir

L'article 135 de la Loi prévoit qu'une personne peut, lorsque sa demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels ou dans le cas où le délai prévu pour répondre est expiré, demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

QUÉBEC

Commission d'accès à
l'information Bureau 2.36
525, boul. René-Lévesque Est
Québec (Québec) G1R 5S9

Tél : (418) 528-7741
Téléc : (418) 529-3102

MONTRÉAL

Commission d'accès à
l'information Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4

Tél : (514) 873-4196
Téléc : (514) 844-6170

b) Motifs

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

APPEL DEVANT LA COUR DU QUÉBEC

a) Pouvoir

L'article 147 de la loi stipule qu'une personne directement intéressée peut porter la décision finale de la Commission d'accès à l'information en appel devant un juge de la Cour du Québec sur toute question de droit ou de compétence.

L'appel d'une décision interlocutoire ne peut être interjeté qu'avec la permission d'un juge de la Cour du Québec s'il s'agit d'une décision interlocutoire à laquelle la décision finale ne pourra remédier.

b) Délais

L'article 149 prévoit que l'avis d'appel d'une décision finale doit être déposé au greffe de la Cour du Québec, dans les 30 jours qui suivent la date de réception de la décision de la Commission par les parties.

c) Procédure

Selon l'article 151 de la loi, l'avis d'appel doit être signifié aux parties et à la Commission dans les dix jours de son dépôt au greffe de la Cour du Québec.

14 juin 2006
Mis à jour le 7 novembre 2020