Chambre de Commerce du Canada | Canadian Chamber of Commerce

Centre de l'avenir des affaires de la Chambre de Commerce du Canada | Canadian Chamber Future of Business Centre

POURQUOI UN CHIFFREMENT FORT

est essentiel pour la sécurité, l'avenir économique et la souveraineté numérique du Canada

Par Heather West et Eric Miller | Juin 2025

Pourquoi un chiffrement fort est essentiel pour la sécurité, l'avenir économique et la souveraineté numérique du Canada par :

Heather West
Membre du Centre de l'avenir des affaires de la Chambre de commerce du Canada
Fellow, Center for Cybersecurity Policy and Law

Eric Miller
Membre du Centre de l'avenir des affaires de la Chambre de commerce du Canada
Président, Rideau Potomac Strategy Group

La Chambre de commerce du Canada a pour mission de préparer l'avenir de la réussite en affaires. Pour faire bouger les choses en matière de politiques publiques avant-gardistes, le Centre pour l'avenir des affaires de la Chambre de Commerce du Canada constitue notre plateforme pour intégrer ces sujets dans le débat public.

Les rapports du Centre sont produits par des chercheurs externes, de manière indépendante, sans lien avec le processus du comité d'orientation de la Chambre de commerce du Canada, fondé sur le consensus. Les opinions exprimées dans ce document sont celles des chercheurs.

Remerciements

Les auteurs tiennent à remercier sincèrement les personnes suivantes qui ont contribué à la réalisation de ce rapport.

Conseil consultatif

Charles Finlay
Directeur exécutif fondateur
Rogers Cybersecure Catalyst,
Toronto Metropolitan University

Daina Proctor
Responsable des services de sécurité canadiens
IBM

Jennifer Quaid
Directrice exécutive
Canadian Cyber Threat Exchange

John Verdi
Premier vice-président aux politiques
Future of Privacy Forum

Mention spéciale

Grace M. O'Neill
Analyste
Center for Cybersecurity Policy and Law

Contenu

« Il n’est pas exagéré de dire qu’un chiffrement fort et une cybersécurité efficace sont devenus des impératifs stratégiques pour le Canada. »

Introduction : Un nouveau – et un ancien – monde

Le Canada de 2025 entre dans une période de profonds changements.

En effet, l'ère de la *Pax Americana* qui a suivi la Seconde Guerre mondiale est largement révolue. Le leadership mondial exercé par les États-Unis a cédé la place à la politique de l'Amérique d'abord. L'administration Trump a entrepris de repenser l'identité de ses alliés. Sur le plan économique, le mouvement de l'Amérique d'abord est synonyme d'imposition généralisée de droits de douane et d'autres restrictions commerciales aux amis traditionnels, comme aux ennemis du pays. Le protectionnisme américain et l'incertitude politique qui émane de Washington sapent le climat d'investissement qui prévaut au Canada, alors que le pays fait depuis longtemps la promotion d'un accès sécurisé au marché américain comme pierre angulaire de son offre. Le Canada cherche désormais authentiquement à diversifier ses échanges commerciaux et à nouer de nouvelles relations avec un sentiment d'urgence sans précédent. Au vu de l'évolution du contexte géopolitique, le Canada, au même titre que d'autres alliés traditionnels des États-Unis, se prépare également à dépenser davantage pour assurer sa propre sécurité en vue de garantir son autonomie stratégique.

Alors que le Canada doit se frayer de nouvelles voies vers son avenir économique, le pays doit être conscient de la dynamique sous-jacente à la création de richesse dans notre monde contemporain. Malgré les tensions géopolitiques croissantes et les évocations de « démondialisation », l'infrastructure numérique qui, au cours du dernier quart de siècle, a assuré l'interconnexion du monde entier par le biais d'ordinateurs et d'appareils, demeure fermement en place et joue un rôle aussi important que jamais dans la vie des citoyens canadiens.

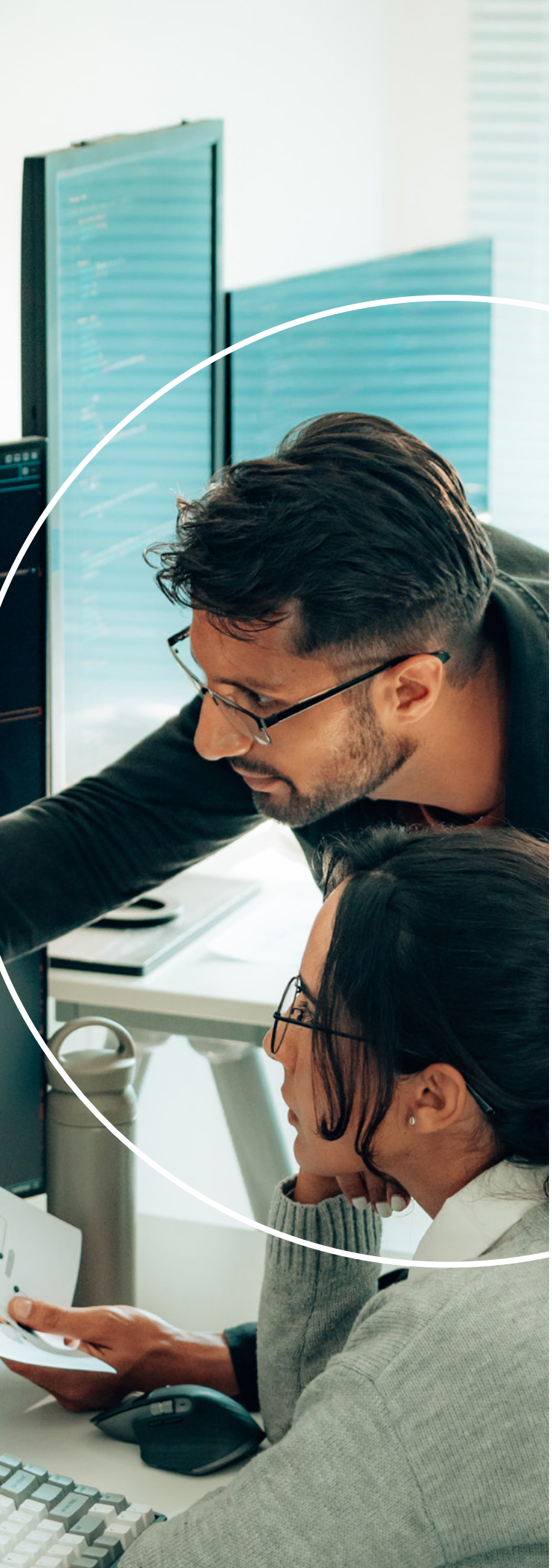
Cette connectivité omniprésente génère d'énormes quantités de données, qui sont devenues en soi un bien précieux. L'économiste canadien Dan Ciuriak note qu'il est difficile d'estimer précisément la valeur de ces données puisqu'il n'existe ni reçu ni facture permettant de fixer une valeur transactionnelle. À titre d'indicateur, il se penche sur la proportion relative des actifs incorporels par rapport aux actifs corporels[1] dans la composition des actifs

1 Les actifs incorporels comprennent les données, les droits d'auteur, les brevets et les marques déposées. Les actifs corporels comprennent les terrains, les bâtiments, les gisements de ressources naturelles et les machines.

des entreprises composant l'indice S&P 500. La part des actifs incorporels est passée de 17 % en 1975 à 68 % en 1995 et à 90 % en 2024. Le Dr Ciuriak scinde ensuite les sous-composantes des actifs incorporels, pour parvenir à estimer que la valeur des données s'élève à 6 300 milliards de dollars, soit 17 % de l'ensemble des actifs incorporels[2].

L'économie numérique a le potentiel d'être un moteur extrêmement puissant de la croissance économique canadienne dans les années à venir. Les Canadiens considèrent trop souvent l'économie numérique comme étant un secteur proprement américain. Il ne fait aucun doute que les États-Unis ont joui de l'avantage du premier dans les années 1990 et jusqu'au cours des années 2010, ce qui a donné naissance à une série d'entreprises technologiques de premier plan au niveau mondial. Il ne fait également aucun doute que la Silicon Valley demeure un lieu de dynamisme économique incroyable. Cependant, le secteur technologique américain n'est pas voué à rester à jamais dominant. En outre, les bouleversements politiques actuels dans des domaines tels que l'immigration pourraient freiner la croissance future du secteur technologique en amenant les innovateurs à s'installer ailleurs. Quoi qu'il en soit, différentes régions du monde ne cessent de créer leurs propres acteurs technologiques de premier plan. Basée à Singapour, la société Grab est devenue si concurrentielle qu'elle est parvenue à évincer Uber du secteur du covoiturage en Asie du Sud-Est. La société Mercado Libre, dont le siège se trouve en Uruguay, est la plus grande entreprise de commerce électronique d'Amérique latine, dominant très largement Amazon dans la région. Spotify, dont le siège se trouve en Suède, est la plus grande entreprise de diffusion de musique en continu au monde. La question politique clé pour les Canadiens devrait être : *Quelles sont les conditions nécessaires à la croissance d'un plus grand nombre d'entreprises technologiques d'envergure mondiale au Canada?*

2 Dr Dan Ciuriak. *Technological Conditions and the Rise and Fall of the Rules-Based System*. SSRN. 23 avril 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4762228 (en anglais).



La politique publique est un élément essentiel de la réponse à cette question. En effet, la prospérité et la sécurité nationale du Canada sont inextricablement liées à la protection de la vie privée et à la cybersécurité dans le domaine numérique. Il peut être difficile d'adopter des politiques équilibrées qui, tout à la fois favorisent l'innovation, sont efficaces sur le plan de leur application et protègent en même temps la vie privée. À travers le monde prévalent une multitude d'approches à l'égard de ces questions. Parvenir à maîtriser la combinaison d'approches la plus judicieuse pour le Canada est fondamental pour que le pays puisse assurer sa réussite dans le nouvel ordre mondial.

À titre de proposition de base, il n'est pas exagéré d'affirmer qu'un chiffrement fort et qu'une cybersécurité efficace sont devenus des impératifs stratégiques pour le Canada. Préparé pour le Centre de l'avenir des affaires de la Chambre de commerce du Canada, le présent rapport politique examine le rôle essentiel que jouent le chiffrement et la cybersécurité au Canada, l'évolution du contexte des menaces, ainsi que les choix politiques auxquels le pays est confronté. Il s'interroge sur les raisons pour lesquelles le maintien d'un chiffrement robuste est essentiel pour la sécurité économique et personnelle, les dangers posés par la cybercriminalité et les faiblesses potentielles du chiffrement, en plus d'examiner la façon dont l'approche du Canada diverge de celle de certains de ses alliés, comme les États-Unis. Le présent rapport examine également les efforts déployés par le Canada pour affirmer une position indépendante, en plus d'analyser en quoi ces efforts cadrent avec la croissance d'un secteur technologique intérieur fort. Pour contextualiser l'approche du Canada, les auteurs ont réalisé des comparaisons avec la situation qui prévaut ailleurs, et notamment dans l'Union européenne et en Australie. Enfin, le présent rapport contient un certain nombre de recommandations pratiques à l'intention des décideurs et des acteurs du monde des affaires afin que puissent être renforcée la cybersécurité du Canada, protégée la vie privée et promue l'innovation.

L’importance cruciale d’un chiffrement fort et de la cybersécurité au Canada

De robustes mesures en matière de chiffrement ou de cryptage et de cybersécurité constituent les pierres angulaires de l’économie canadienne, des opérations gouvernementales et de la protection de la vie privée à l’ère numérique. Elles fournissent aux citoyens, aux consommateurs, aux entreprises et aux gouvernements la confiance et la sécurité nécessaires pour que les opérations et les communications numériques puissent se dérouler comme il se doit.

Protéger l’économie et le commerce

Le chiffrement sécurise le vaste éventail d’activités économiques qui sont désormais menées en ligne – des opérations bancaires au commerce électronique en passant par l’échange de propriété intellectuelle. Le chiffrement protège les secrets commerciaux, les stratégies commerciales et les données des clients contre l’espionnage industriel ou le vol[3]. Comme la plupart des entreprises canadiennes font partie des rangs des petites et moyennes entreprises (PME), leur capacité à livrer concurrence et à innover est souvent tributaire d’un accès abordable à un chiffrement fort et à des réseaux sécurisés. Affaiblir délibérément le chiffrement mis à la disposition des entreprises

3 https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cyber security-economic-growth-and-foreign-policy/#:~:text=Encryption%20is%20used%20to%20protect,the%20trust%20of%20their%20customers (en anglais).

ou de leurs clients saperait directement leur croissance, en plus d'éroder la confiance des clients[4]. Les Canadiens dépensent aujourd'hui environ 100 milliards de dollars canadiens par an en commerce électronique de détail. Ces transactions ne sont rendues possibles que grâce à des systèmes de paiement cryptés qui permettent aux consommateurs de compter sur le maintien de la confidentialité des renseignements relatifs à leurs cartes de crédit ainsi que de leurs renseignements personnels. Sans chiffrement et cyberprotection, il y a fort à parier que la remarquable croissance de l'économie numérique s'essoufflerait en raison d'un manque de confiance.

Sécuriser les opérations gouvernementales et les infrastructures essentielles

Les gouvernements fédéral, provinciaux et municipaux s'appuient sur le chiffrement pour tout sécuriser ou protéger, des communications classifiées et des dossiers des citoyens jusqu'aux contrôles des infrastructures essentielles. Les infrastructures de communication – y compris les systèmes de télécommunications, de transport, d'énergie et financiers – ont toutes recours au chiffrement pour préserver leur intégrité et prévenir toute intrusion malveillante. Sécurité publique Canada note que « Le chiffrement vise à protéger l'intégrité des infrastructures essentielles nationales de l'intrusion malveillante. Le chiffrement touche à tout en ce qui concerne entre autre les systèmes de télécommunication et de transports, le secteur de l'énergie et les services financiers. »[5]. La cybersécurité du gouvernement est la sécurité

4 Ibidem.

5 https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/035/index-fr.aspx?wbdisable=true

nationale : des réseaux chiffrés protègent les communications militaires et les services de renseignement, tandis que les défenses en matière de cybersécurité empêchent les acteurs hostiles de saboter les infrastructures essentielles du pays ou de subtiliser des données sensibles. Le gouvernement du Canada a un double intérêt, soit avoir recours à un chiffrement fort à l'interne pour protéger ses opérations, d'une part, et promouvoir des normes de cybersécurité élevées au niveau de l'ensemble de la société canadienne afin de rendre le pays moins vulnérable et plus prospère, d'autre part.

Protéger la vie privée et les renseignements personnels

Pour les particuliers, le chiffrement constitue souvent la dernière ligne de défense protégeant les communications et les renseignements personnels. À une époque où les Canadiens confient leurs données médicales, leurs dossiers financiers et leurs conversations quotidiennes à des services numériques, le chiffrement permet de garantir que ces renseignements de nature sensible demeurent confidentiels et ne soient accessibles qu'aux personnes concernées. Le chiffrement de bout en bout des applications de messagerie, par exemple, permet aux Canadiens de communiquer en privé sans crainte d'être écoutés – ce qui s'avère être une nécessité contemporaine pour exercer le droit fondamental à la vie privée. Bien que la *Charte canadienne des droits et libertés* ne comprenne pas un droit spécifique à la vie privée, les tribunaux ont interprété le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives de l'article 8 comme une solide protection de la vie privée dans le domaine des communications. La Cour suprême du Canada a affirmé à plusieurs reprises que les particuliers ont des attentes raisonnables en matière de vie privée dans leurs communications numériques, rejetant en cela l'approche américaine plus « permissive » qui nie la protection de la vie privée dans le cas des données partagées avec un tiers[6]. Le chiffrement soutient donc en ce sens les droits prévus en vertu de la Charte en intégrant techniquement le respect de la vie privée dans le domaine numérique. Il soutient également la liberté d'expression et d'association. En 2020, ce sont bien les gouvernements du Groupe des cinq[7], dont le Canada, qui publièrent un document intitulé *Déclaration internationale : chiffrement de bout en bout et sécurité publique*. On y retrouve ce qui suit : « … le chiffrement hautement sécurisé, lequel joue un rôle crucial dans la protection des données personnelles, de la vie privée, de la propriété intellectuelle, des secrets commerciaux et de la cybersécurité » et « est une ancre de confiance primordiale dans le monde numérique »[8]. En d'autres termes, le chiffrement fort sous-tend l'existence du Canada en tant que société libre et le statut des Canadiens en tant que peuple libre.

Le chiffrement fort et la cybersécurité ne constituent pas des préoccupations de niche des ingénieurs de réseaux numériques. Ce sont plutôt les pierres angulaires de la sécurité, de la prospérité et de la protection de la vie privée.

6 https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/#:~:text=In%20contrast%2C%20that%20potential%20seedling,the%20same%20types%20of%20personal (en anglais).

7 Le Groupe des cinq s'entend du réseau de partage de renseignements composé des gouvernements du Canada, des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande.

8 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2020-jnt-sttmnt-ncrptn-pblc-sfty/index-fr.aspx

La croissance des cybermenaces dans une économie et une société mondiales numérisées

Au cours des 25 dernières années, tout s'est numérisé. Il n'est donc pas surprenant que les criminels, les propagandistes et les espions de nations hostiles passent désormais une grande partie de leur temps dans le cyberespace. Les plateformes de vente au détail en ligne permettent aux Canadiens d'accéder à des marchandises provenant des quatre coins du monde. Cependant, ces mêmes liens de connectivité exposent la vie des Canadiens à des périls du monde entier. La sécurité et la confiance n'ont jamais été aussi importantes qu'aujourd'hui.

Hausse de la cybercriminalité

Pour les malfaiteurs, nous vivons actuellement l'« âge d'or » de la cybercriminalité. Ces criminels ont continué à se multiplier parce qu'ils peuvent désormais réaliser des profits importants tout en courant peu de risques d'être arrêtés, notamment lorsqu'ils opèrent à l'étranger. Certains États-nations ont même conclu une forme de partenariat public-privé avec des gangs de criminels. Le document intitulé Évaluation des cybermenaces nationales 2023-2024 (ECMN) du Centre canadien pour la cybersécurité considère que les rançongiciels constituent la forme de cybercriminalité la plus susceptible d'avoir une incidence sur les organisations et les particuliers canadiens[9]. En 2021, furent dénombrées au moins 235 attaques avérées au moyen de rançongiciels envers l'industrie canadienne – ce qui représente une moyenne de près de cinq attaques de ce genre par semaine –, chaque incident coûtant en moyenne 6,35 millions de dollars en frais de reprise et en occasions perdues[10].

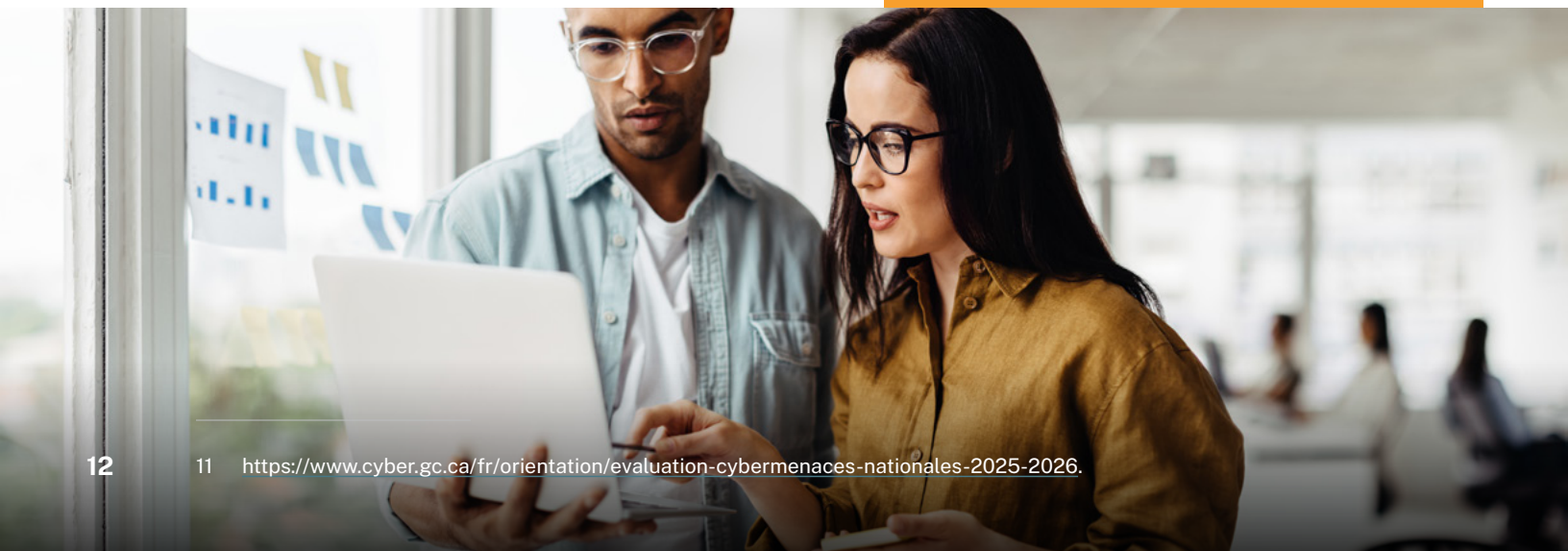
9 https://www.cyber.gc.ca/sites/default/files/ecmn-2023-24-web2.pdf.

10 https://www.cigionline.org/articles/inadequate-cyber-defence-is-damaging-canadas-economy/#:~:text=Incidents%20such%20as%20these%20may,attacks%3B%20most%20were%20launched%20by (en anglais).

Menaces pour les infrastructures essentielles

Dans une économie numérisée, les infrastructures essentielles constituent une cible de choix pour les cybercriminels et pour les pirates informatiques parrainés par un État. Les attaques incessantes à l'encontre du réseau électrique ukrainien rappellent l'ampleur des destructions que les cyberarmes peuvent causer aux principaux systèmes opérationnels de la société. Le Canada n'est certainement pas à l'abri de cela. En effet, des secteurs tels que la finance, l'énergie, les transports et la santé ont subi des cyberincidents majeurs. Des groupes de cybercriminels ciblent des opérateurs d'infrastructures essentielles en sachant que leurs perturbations peuvent être plus préjudiciables et mener à des versements plus rapides de rançons. Ainsi, à titre d'exemple, une attaque visant un pipeline ou un service d'électricité peut interrompre la prestation de services à des millions de personnes. Les pays hostiles ciblent les infrastructures essentielles à la fois à des fins d'espionnage et du fait du vaste potentiel de destruction advenant une guerre. Le Centre de la sécurité des télécommunications Canada (CST) – soit l'agence canadienne de renseignement d'origine électromagnétique (SIGINT) et de cyberdéfense – considère qu'il parvient à bloquer annuellement des milliards de cyberactions ciblant des systèmes gouvernementaux. Le tableau d'ensemble est celui de menaces « complexes et sophistiquées » nécessitant que l'on fasse preuve d'une vigilance de tous les instants[11].

L'environnement sur le plan des cybermenaces auquel est confronté le Canada et les Canadiens est redoutable. Les cyberattaques représentent un danger clair et présent pour la prospérité économique et la sécurité publique du Canada de même que pour le bien-être de ses citoyens. Cette réalité justifie l'importance considérable accordée par le Canada à la cybersécurité. Elle situe également le contexte essentiel des débats concernant le chiffrement et l'accès légal – l'augmentation de la criminalité et les attaques difficiles à retracer étant souvent citées par les responsables de l'application de la loi comme une raison de demander plus de pouvoirs, y compris sur le plan de l'accès aux données chiffrées.



11 https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026.

L’affaiblissement du chiffrement fait peser des risques importants sur les intérêts canadiens

Face à la montée de la cybercriminalité et aux préoccupations en matière de sécurité nationale, certaines voix – qui sont souvent celles des représentants de la police ou des services de renseignement – ont proposé que soient affaiblies les protections en matière de chiffrement afin de faciliter l’accès aux données.

Cette approche est généralement désignée par les formules « accès exceptionnel » ou « accès légal ». Plus précisément, il s’agirait en l’espèce de demander aux entreprises technologiques d’intégrer à leurs services chiffrés des portes dérobées ou d’exiger que les clés de chiffrement des utilisateurs soient mises sous séquestre de telle sorte que le gouvernement puisse les obtenir en cas de besoin. Bien que l’objectif soit d’aider les représentants des forces de l’ordre à attraper les criminels, voire à prévenir les attaques terroristes, de telles mesures présenteraient de graves risques pour les intérêts du Canada en matière d’économie, de sécurité et de liberté civile. En effet, intégrer des portes dérobées aux systèmes constitue en quelque sorte une invitation ouverte faite aux auteurs de menace à en tirer parti. Pratiquement tous les experts du domaine de la cybersécurité de même que toutes les grandes entreprises technologiques s’accordent à dire que l’affaiblissement délibéré du chiffrement nuit à la sécurité de tous et ne vaut pas le prétendu compromis en matière de sécurité publique. En outre, l’existence de portes dérobées saperait la confiance des utilisateurs et des clients à l’égard des produits et services canadiens. Il ne s’agit pas là d’une façon avisée de se doter d’un secteur numérique concurrentiel au niveau mondial.

Ce que disent les lois canadiennes sur la cybercriminalité et l'accès légal

Le droit criminel canadien traite du chiffrement de manière indirecte, principalement dans le contexte de l'accès légal à l'information.

La partie VI du *Code criminel* régit la question de l'interception d'une communication privée (écoute téléphonique) et exige généralement des services policiers qu'ils obtiennent l'autorisation d'un juge (mandat) pour intercepter une communication. Ces dispositions relatives à l'interception s'appliquent à toutes les communications, qu'elles soient ou non chiffrées.

La loi ne prévoit aucune exception qui modifierait l'obligation d'obtenir un mandat du fait que la communication est chiffrée. En d'autres termes, les services policiers ne disposent d'aucune autorité supplémentaire sur le plan de l'interception et ils doivent toujours respecter le seuil élevé fixé pour obtenir un mandat de mise sous écoute électronique prévu en vertu de la partie VI si une communication est interceptée légalement mais est chiffrée. Par exemple, si des enquêteurs mettent sous écoute un flux de messagerie chiffré de bout en bout (E2EE), la loi autorise cette interception, mais n'oblige pas le fournisseur de services à en déchiffrer le contenu. Contrairement à ce qui est le cas dans certains pays, le Canada n'a pas de loi qui contraint les entreprises technologiques à veiller à ce que leurs systèmes soient déchiffrables. Par conséquent, les messages chiffrés de bout en bout interceptés alors qu'ils sont en transit demeurent parfaitement incompréhensibles pour les autorités, à moins qu'elles ne soient en mesure de les déchiffrer elles-mêmes.

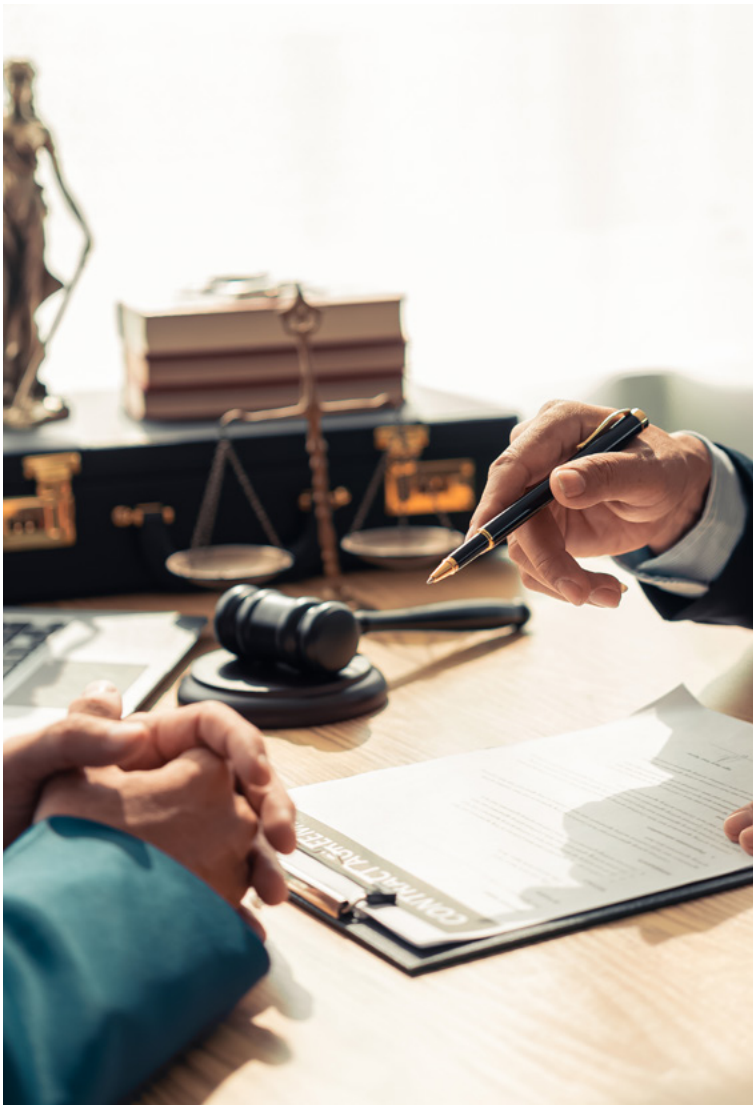
Est cependant prévue une exception importante dans le cas de la réglementation relative aux fournisseurs de télécommunications titulaires d'une licence. Depuis 1995, les *Normes d'application du Solliciteur général sur l'interception licite des télécommunications* (NASG) imposent des exigences techniques aux entreprises de télécommunications sans fil, comme condition d'obtention d'une licence. La norme 12 des NASG exige en effet des entreprises de télécommunications qu'elles fournissent les communications chiffrées réalisées sur leur réseau aux responsables de l'application de la loi « en clair » (c.àd. non chiffrées) sur demande légitimement formulée en ce sens. Cette mesure a pour effet de les dissuader d'avoir recours à l'égard du trafic voix/données à quelque forme de chiffrement que ce soit qu'ils ne soient pas en mesure de

déchiffrer pour les responsables de l'application de la loi. Dans le cas des services basés sur Internet (applications de messageries, voix sur IP, etc.), il n'existe aucune réglementation canadienne équivalente imposant la conception du chiffrement. Comme les entreprises actives dans les domaines d'Internet et de la technologie ne sont généralement pas soumises aux conditions propres à celles des entreprises de télécommunications titulaires d'une licence, les services E2EE (p. ex. WhatsApp, iMessage, BlackBerry Messaging) ne sont pas liés par les NASG et peuvent dès lors prévoir librement un chiffrement fort.

Outre l'interception en temps réel, le *Code criminel* prévoit l'obtention d'un mandat de perquisition et d'ordonnances de communication pour obtenir des données stockées. Ces mandats et ordonnances peuvent viser des informations chiffrées. À titre d'exemple, la police peut saisir un appareil chiffré ou contraindre un fournisseur Internet à lui remettre des données chiffrées. Cependant, la loi canadienne n'oblige pas le destinataire d'une telle ordonnance à déchiffrer les données ou à en révéler une clé de chiffrement s'il n'est pas déjà en possession du texte en clair. Si la *Loi sur la protection des Canadiens contre la cybercriminalité* (2014) a élargi ces pouvoirs d'enquête (en ajoutant les ordres et les ordonnances de conservation et en actualisant les pouvoirs en matière d'ordonnances de communication), elle n'a pas pour autant créé de nouvelles obligations d'assistance au chapitre du déchiffrement.

Le droit canadien criminalise certaines cyberactivités liées au chiffrement dans des contextes spécifiques. Par exemple, il est illégal d'intercepter délibérément des communications privées sans autorisation légale, de sorte que le piratage du flux de communications chiffré d'une personne constitue un délit. La possession ou l'utilisation d'un dispositif permettant d'obtenir frauduleusement des services informatiques constitue également un délit. En théorie, l'utilisation malveillante d'outils de craquage de chiffrement pourrait être visée, bien que la loi cible les dispositifs de piratage de manière plus générale. Fait à noter, le recours au chiffrement pour dissimuler les preuves d'un délit n'est pas en soi un délit. Si une personne détruisant des preuves peut se voir accusée d'entrave à la justice, le simple fait de chiffrer ses fichiers ou ses communications est un acte légal, même s'il a pour effet d'entraver les enquêteurs.

Le *Code criminel* permet à un juge qui délivre un mandat ou une autorisation d'écoute électronique d'ordonner à un tiers d'aider les services policiers à l'exécuter en vertu d'une ordonnance d'assistance d'« accès légal ». Des procureurs ont tenté d'avoir recours à cette



disposition pour obtenir de façon forcée une assistance en matière de déchiffrement (p. ex. en ordonnant à un suspect ou à une entreprise de technologie d'apporter son aide pour déverrouiller un appareil). À ce jour, aucune loi canadienne n'oblige explicitement une personne à dévoiler son mot de passe ou sa clé de chiffrement, et les tentatives en ce sens se sont heurtées à des obstacles constitutionnels. Dans un arrêt de 2010 de la Cour d'appel du Québec, le tribunal a affirmé que le fait de forcer une personne à révéler son mot de passe était inadmissible et que toute donnée obtenue ainsi constituerait une saisie « déraisonnable » – la loi n'autorise pas une ordonnance qui, dans les faits, contraint une personne à s'auto-incriminer. De même, dans l'affaire *R. c. Shergill* (2019), un tribunal de l'Ontario a refusé de faire exécuter une ordonnance d'assistance contre un accusé pour l'obliger à déverrouiller son téléphone, en venant à la conclusion que le fait d'exiger un mot de passe violerait le droit de ne pas s'auto-incriminer garanti par la Charte. Ces affaires soulignent qu'en vertu de la *Charte canadienne des droits et libertés*, un accusé a le droit de ne pas être contraint de participer à la poursuite qui est engagée contre lui [l'article 7 et l'alinéa 11c) de la Charte prévoient des protections contre l'auto-incrimination et le fait d'être forcé à témoigner contre soi-même].

Pour les tiers comme les entreprises, le droit est moins clairement établi. En effet, une ordonnance d'assistance pourrait éventuellement contraindre une entreprise technologique à apporter son aide (p. ex. en tentant un déchiffrement, pour autant que cela soit possible); cependant, comme la plupart des fournisseurs d'E2EE ne détiennent pas les clés, ils n'ont pas la capacité de s'y conformer. En l'état actuel des choses, aucune loi n'oblige clairement une entreprise technologique à élaborer un outil de déchiffrement ou une porte dérobée pour les enquêteurs. Toute demande en ce sens donnerait également probablement lieu à une contestation en vertu de la Charte, en invoquant le droit à la vie privée prévu en vertu de l'article 8 de même que le droit à la liberté d'expression, si elle prévoyait l'obligation d'écrire du code. En pratique, les services policiers canadiens ont parfois trouvé des solutions créatives. Dans un cas en particulier, la Gendarmerie royale du Canada (GRC) a obtenu une clé de chiffrement principale BlackBerry par des moyens non divulgués et s'en est servie pour déchiffrer plus d'un million de messages au cours d'une enquête criminelle. Cependant, de tels cas sont rares et souvent entourés du plus grand secret. En droit criminel, en définitive, le chiffrement est donc reconnu comme un obstacle que les services policiers doivent surmonter en tenant compte des pouvoirs dont ils disposent actuellement. Le fait que les données chiffrées d'une entreprise technologique puissent constituer un obstacle à l'application de la loi n'est pas réglementé par une loi anti-chiffrement spéciale.

Dans le secteur plus vaste des infrastructures essentielles et du gouvernement, le chiffrement est dans une large mesure perçu comme constituant une mesure de sécurité positive. Les politiques en matière de cybersécurité du Canada encouragent le recours à un chiffrement robuste pour protéger les systèmes essentiels des cybermenaces, comme dans le cas des réseaux bancaires, d'énergie et de transport. À titre d'exemple, la Stratégie nationale de cybersécurité du gouvernement du Canada ainsi que les orientations du Centre canadien pour la cybersécurité préconisent l'adoption de normes cryptographiques strictes pour sécuriser les données et les communications sensibles dans le contexte des systèmes essentiels. Dans les secteurs réglementés, les autorités recommandent ou exigent souvent le recours au chiffrement par le biais de normes. À titre d'exemple, les institutions financières qui relèvent du Bureau du surintendant des institutions financières (BSIF) sont censées chiffrer les données et les transactions des clients, respectant en cela les lignes directrices en matière de gestion des cyberrisques du BSIF. Dans le secteur des soins de santé, comme nous l'avons indiqué plus tôt, les responsables de la réglementation insistent sur le chiffrement des renseignements relatifs au patient.

Facteurs géopolitiques et l'effritement du Groupe des cinq

L'alliance du Groupe des cinq est un pilier de l'architecture de sécurité du monde démocratique depuis deux décennies. L'alliance repose sur la confiance et les valeurs partagées – qui semblent aujourd'hui s'effriter.

L'origine du Groupe des cinq remonte à la coopération en matière de sécurité entre les alliés pendant la Seconde Guerre mondiale. S'étant vu accorder une autonomie complète par rapport à la Grande-Bretagne en vertu du *Statut de Westminster de 1931*, le Canada a affirmé l'indépendance de sa politique étrangère en déclarant séparément la guerre à l'Allemagne en septembre 1939. Tout au long du conflit, le Canada mit en place et fournit des capacités distinctes pour soutenir la cause des alliés. En juin 1941, le Canada créa la Sous-section de l'examen (XU) – son premier bureau civil de cryptographie – sous les auspices du Conseil national de recherches du Canada (CNRC)[12]. La Sous-section de l'examen joua un rôle clé dans les efforts déployés par les alliés pour décrypter les codes et les clés de chiffrement ennemis utilisés dans les signaux de communication de 1941 à 1945. La Sous-section de l'examen remporta des succès importants, alors qu'elle put notamment décrypter des codes et résoudre le chiffrement par transposition utilisé par la flotte de Vichy[13].

À la fin de la guerre, les dirigeants canadiens décidèrent de maintenir un bureau civil de cryptographie. Ils avaient bien saisi la valeur que représentait un organisme gouvernemental spécialisé se consacrant à la protection des informations sensibles, ce qui représentait un besoin de plus en plus important. La Direction générale des communications du CNRC commença ses activités en 1946, son personnel se composant d'ex-employés de la Sous-section de l'examen. Le travail de la XU mené en temps

12 Voir le texte à : https://www.canada.ca/fr/parcs-canada/nouvelles/2021/08/la-sous-section-de-lexamen-1941-1945.html.

13 Voir le texte à : https://parcs.canada.ca/culture/designation/evenement-event/examen-examination.

de guerre s'était avéré essentiel pour jeter les bases des capacités du Canada en matière de renseignement d'origine électromagnétique en temps de paix, pour assurer la position du Canada dans les négociations d'après-guerre sur le renseignement, ainsi que pour contribuer à faire de la cryptographie une fonction clé du gouvernement fédéral[14]. En 1975, la Direction générale des communications fut rebaptisée Centre de la sécurité des télécommunications (CST)[15], lequel relèverait désormais du ministre de la Défense nationale.

L'alliance en matière de partage de renseignements du Groupe des cinq est le fruit d'une série d'accords. Ce partenariat naquit de la collaboration fructueuse menée entre les États-Unis et la Grande-Bretagne en matière de renseignement pendant la guerre. En 1949, Ottawa et Washington signaient l'entente de CANUSA[16]. L'alliance fut élargie à l'Australie et à la Nouvelle-Zélande en 1956[17]. Tout au long de la Guerre froide, ce solide réseau de confiance se révéla incroyablement efficace et durable.

Après la Guerre froide, les activités de renseignement d'origine électromagnétique du Canada, au même titre que celles de ses alliés, furent appelées à évoluer avec le temps. Avec le début de la guerre en Afghanistan en 2001, le CST fut appelé, pour la première fois depuis la guerre de Corée, à soutenir les troupes en situation de combat. De son propre aveu, le CST a fourni la moitié des renseignements portant sur les militants et les chefs talibans, de même que sur leurs stratégies utilisés par l'armée canadienne pendant la guerre. Une bonne partie du reste des renseignements provenaient de ses partenaires en matière de renseignement, et notamment du Groupe des cinq. Manifestement, le Canada fut appelé à fournir de nombreux renseignements exploitables à ses alliés ayant des troupes sur le terrain. En 2016, le CST joua un rôle essentiel, y compris en parvenant à pirater des systèmes informatiques dans le cadre de l'opération Impact, soit la mission des Forces armées canadiennes contre ISIS[18].

En outre, le CST est parvenu à suivre les évolutions technologiques. Avec l'essor d'Internet, les activités de renseignement d'origine électromagnétique passaient de moins en moins par les appels téléphoniques et de plus en plus en ligne. En 2000, le CST s'est fixé une nouvelle mission : « être l'agence qui maîtrise le réseau mondial d'information pour améliorer la sécurité et la prospérité du Canada » [Traduction][19]. En 2001, à la suite des attentats du 11 septembre, le gouvernement du Canada adopta la *Loi antiterroriste*, qui contribua en fait à concrétiser cette vision. Elle permit au CST d'étendre considérablement ses activités de surveillance numérique et d'organiser une solide cyberdéfense[20]. Au milieu des années 2010, il n'était pas rare que l'on entende dire que les capacités en matière de cybersécurité et de renseignement numérique du CST étaient bien supérieures à ce à quoi on aurait normalement dû s'attendre au vu de son budget. En 2018, le gouvernement du Canada créa le Centre canadien pour la cybersécurité, pour faire face aux menaces pesant sur les réseaux gouvernementaux et sur ceux de l'ensemble du pays[21].

14 Voir le texte à : https://www.canada.ca/fr/parcs-canada/nouvelles/2021/08/le-gouvernement-du-canada-reconnait-le-bureau-civil-de-cryptographie-de-la-seconde-guerre-mondiale-comme-un-evenement-historique-national.html.

15 Voir le texte à : https://www.cse-cst.gc.ca/fr/culture-et-communaute/histoire.

16 Voir le texte à : https://www.cips-cepi.ca/2020/10/21/the-changing-scope-of-the-five-eyes-implications-for-canada/ (en anglais).

17 Voir le texte à : https://direct.mit.edu/jcws/article/25/1/101/115125/Why-the-Five-Eyes-Power-and-Identity-in-the (en anglais).

18 Murray Brewster. *Canada's electronic spy service to take more prominent role in ISIS fight*. CBC News. 18 février 2016. https://www.cbc.ca/news/politics/canada-spy-agency-isis-fight-1.3454617 (en anglais).

19 Bill Robinson. *Marking 70 years of eavesdropping in Canada*. OpenCanada. 1er septembre 2016. https://opencanada.org/marking-70-years-eavesdropping-canada/ (en anglais).

20 *Partie II : Évolution du cadre de cyberdéfense du gouvernement du Canada*. Comité des parlementaires sur la sécurité nationale et le renseignement. 14 février 2022. https://nsicop-cpsnr.ca/reports/rp-2022-02-14/04-fr-partie-2.html.

21 Ibidem.

L'effritement de l'alliance que représente le Groupe des cinq constitue une tragédie pour toutes les parties en cause. Cependant, un rétablissement de cette alliance dans le climat politique qui prévaut actuellement semble délicat. L'administration Trump présente généralement ses alliés traditionnels les plus proches comme des « profiteurs » qui « arnaquent » les États-Unis. Les droits de douane imposés par le président Trump et ses déclarations quasi incessantes portant sur son désir d'annexer le Canada ont empoisonné les relations avec les États-Unis. En février 2025, le Financial Times indiquait que Peter Navarro, un influent conseiller commercial du président Trump, faisait pression pour que le Canada soit retiré du Groupe des cinq à titre de moyen pour exercer une pression sur l'économie canadienne[22]. Bien que Peter Navarro ait démenti cette information, elle cadre néanmoins avec l'approche du président Trump en matière de politique étrangère, qui consiste à faire l'impasse sur huit décennies de confiance et de partenariat pour obtenir un effet de levier à court terme.

En définitive, cela signifie que le Canada devra réduire sa dépendance à l'égard des échanges de renseignement avec les États-Unis et créer d'autres partenariats adaptés aux réalités de notre époque, tout en investissant considérablement dans le renforcement de ses propres capacités.

22 https://www.ft.com/content/2dfa3c11-64a7-49f6-83df-939b8d1cfb8e (en anglais).

Outre le « facteur Trump », les pays membres du Groupe des cinq ont également divergé à l'égard de certaines questions politiques clés, au rang desquelles figurent l'accès légal ainsi que la surveillance et la protection de la vie privée.

Accès légal : Les États-Unis, le Royaume-Uni et l'Australie ont eu tendance à former une cohorte plus ferme en faveur d'un « accès légal » à l'égard des communications chiffrées. Bien qu'ils se soient généralement montrés favorables, la Nouvelle-Zélande et le Canada ont adopté une approche plus discrète et ont fait preuve de plus de modération dans leur rhétorique. En 2016, le Royaume-Uni a adopté l'*Investigatory Powers Act*, de portée très large, qui comprend des dispositions permettant, sous couvert d'un mandat, la suppression des protections électroniques (c.àd. du chiffrement). Pour sa part, en 2018, l'Australie a adopté une loi anti-chiffrement très générale qui contraint les entreprises à aider les autorités à accéder aux données chiffrées. Par opposition, si le Canada a souscrit à un texte exhortant les entreprises technologiques à trouver des solutions pour permettre au gouvernement d'accéder aux données chiffrées, cette approche ne s'est pas pour autant transposée au niveau de ses lois nationales.

Surveillance : Tel qu'indiqué ci-dessus, les tribunaux américains adhèrent à la « doctrine du tiers », selon laquelle toute information communiquée volontairement à un tiers, comme à une banque, à une société de télécommunications ou à un fournisseur de services en ligne, ne bénéficie d'aucune protection de la vie privée prévue en vertu du 4e amendement à la Constitution des États-Unis. Citizen Lab estime que cette approche a permis aux autorités américaines de réaliser la plus vaste collecte de données, sans mandat, depuis les années 1970[23]. Par opposition, la jurisprudence canadienne a rejeté cette doctrine. La Cour suprême du Canada a indiqué en guise d'avertissement que toute surveillance électronique non assujettie à des restrictions « rend possible [...] l'anéantissement de tout espoir que nos communications restent privées » et qu'elle nécessitait donc une stricte surveillance[24]. En conséquence, le droit canadien impose davantage de contraintes à l'accès par les responsables de l'application de la loi aux données (mandats, ordonnances judiciaires, etc.) et considère le respect de la vie privée comme un droit quasi constitutionnel, même dans un contexte numérique. Cette divergence signifie que certaines pratiques américaines comme celle qui prévoit le recours à des citations à comparaître à large portée pour obtenir des métadonnées sur Internet ou que les dispositions du *Patriot Act* seraient probablement jugées inconstitutionnelles au Canada. Plus généralement, les États-Unis n'ont pas de régime national en matière de protection de la vie privée. Le Canada, pour sa part, dispose d'un tel régime, qui se fonde sur des lois fédérales et provinciales, de même que sur des institutions telles que le Commissariat à la protection de la vie privée (voir l'annexe A pour retrouver un aperçu plus détaillée du régime canadien). Cette différence au chapitre de la philosophie crée régulièrement des tensions au sujet des flux de données transfrontaliers et de la coopération.

23 https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/#:~:text=are%20more%20incompatible%20when%20it,law%20enforcement (en anglais).

24 Ibidem.

Faire cadrer les efforts concernant la protection de la vie privée et la sécurité avec la croissance du secteur technologique et de strictes normes en matière de chiffrement

Les approches du Canada en ce qui concerne les politiques de protection de la vie privée, de chiffrement et de cybersécurité ne se développent pas en vase clos. Au contraire, ces approches recoupent directement – et façonnent tout autant – l'ambition économique que caresse le pays de favoriser l'établissement d'un secteur technologique intérieur de calibre mondial. Plutôt que de percevoir la sécurité et la protection de la vie privée comme constituant des fardeaux pour l'industrie, le Canada les considère de plus en plus comme des facteurs de différenciation susceptibles de stimuler l'innovation et la croissance.

La confiance à titre d'avantage concurrentiel

Sur le marché du numérique, la confiance est une monnaie d'échange. En effet, les entreprises aptes à garantir aux utilisateurs et aux clients que leurs données sont sécurisées et traitées de manière responsable peuvent se forger un avantage concurrentiel notable. Fort de lois strictes sur la protection de la vie privée et d'une réputation enviable en matière de sécurité, le Canada se positionne à titre de nation offrant un niveau de confiance considérable. À titre d'exemple, cela pourrait inciter des entreprises à mener des recherches sur l'intelligence artificielle (IA) au Canada, sachant que le cadre réglementaire respecte la vie privée et évite les « complexités inhérentes » à des nations telles que les États-Unis et la Chine. Cela pourrait également constituer un argument de vente pour les entreprises technologiques canadiennes cherchant à se développer à l'échelle mondiale,

alors qu'elles pourraient faire valoir que leurs produits sont élaborés et mis à l'épreuve dans l'un des régimes de protection de la vie privée les plus stricts au monde, ce qui serait en soi attrayant pour les consommateurs et les entreprises soucieux de la protection de la vie privée, notamment en Europe et en Asie. Par exemple, une entreprise canadienne œuvrant dans le domaine du logiciel qui se conforme d'entrée de jeu au Règlement général sur la protection des données (RGPD) européen pourrait plus facilement commercialiser ses produits sur les marchés internationaux qu'un concurrent américain qui pourrait être tenu de se mettre en conformité après coup. Si le Canada continue à militer en faveur du chiffrement (veillant ainsi à ce que les communications professionnelles, le stockage dans le nuage, etc. soient sécurisés), il instaurera un milieu dans lequel les entrepreneurs numériques pourront élaborer des services sans avoir à constamment s'inquiéter que leur modèle d'affaire soit mis en péril par des atteintes. L'existence de normes de chiffrement élevées est également synonyme d'une réduction du nombre de cyberincidents dévastateurs, ce qui fait du Canada un endroit stable pour faire des affaires. En bref, le refus du Canada d'affaiblir le chiffrement pourrait en fait attirer les entreprises qui souhaitent promettre la sécurité à leurs clients.

Adopter de rigoureuses normes mondiales – Une stratégie de diversification des échanges

Le fait que le Canada adopte de strictes normes en matière de protection de la vie privée et de chiffrement facilite également la tâche de ses entreprises, s'agissant pour ces dernières d'exercer leurs activités et de se développer à l'échelle internationale. Par exemple, l'adoption de normes similaires au RGPD signifie que les entreprises canadiennes sont déjà conformes ou le sont pratiquement lorsqu'elles pénètrent sur le marché européen. De la même façon, en militant en faveur du chiffrement, les applications ou les dispositifs de communication canadiens ne seraient pas considérés avec suspicion dans les régions où prévalent de strictes lois sur la protection de la vie privée. Alors que d'autres pays et régions s'emploieront à rehausser leurs normes (étant acquis que même l'industrie technologique américaine tend à hausser le niveau de protection de la vie privée en raison de la demande des consommateurs et de la réglementation des États), les entreprises canadiennes s'étant développées dans un contexte prévoyant des attentes élevées en matière de protection de la vie privée et de sécurité jouiront d'une longueur d'avance.

Développer les talents et les compétences

Le développement du secteur de la cybersécurité de même que celui du secteur technologique au sens large sont confrontés au Canada à une énorme pénurie de compétences[25]. Les efforts à ce chapitre signifieraient qu'il faudrait former la prochaine génération de travailleurs qualifiés qui puisse contribuer à la fois à la sécurité et à l'innovation. Le gouvernement et le secteur privé collaborent à des initiatives qui visent à combler la pénurie de talents en matière de cybersécurité, alors qu'ils financent davantage de programmes universitaires, qu'ils créent des environnements de formation de type « Cyber Range » et soutiennent des initiatives visant à amener des groupes sous-représentés vers le domaine de la technologie, élargissant du même coup le bassin de talents. Le développement d'un secteur technologique intérieur robuste nécessite que l'on puisse compter sur une solide réserve d'ingénieurs, de développeurs et de chercheurs. En rendant la cybersécurité « sympathique » et en faisant une priorité, ce qui pourrait être facilité par l'accent mis dans la population sur l'importance de la sécurité nationale et d'une vision d'ensemble, un plus grand nombre d'étudiants pourraient se tourner vers ces domaines. La Chambre de commerce du Canada et les entreprises pourraient s'associer aux universités pour offrir des stages et des stages en milieu de travail dans le domaine de la sécurité et de la protection de la vie privée, ce qui permettrait de faire cadrer les résultats au niveau pédagogique avec les besoins de l'industrie. En outre, si le Canada est perçu comme offrant un environnement favorable à la protection de la vie privée et à la sécurité, il pourrait être en mesure de retenir des talents, qui pourraient autrement choisir d'aller s'installer dans la Silicon Valley – étant acquis que certains travailleurs du domaine de la technologie choisissent leurs employeurs et leurs pays en fonction de la mesure dans laquelle leurs visées sont communes aux leurs. Par exemple, un cryptographe ou un éthicien de l'IA compétents pourraient préférer travailler au Canada, où le cadre juridique correspond à leurs valeurs, plutôt que dans un autre pays où ils estiment que leur travail pourrait servir à des activités de surveillance de masse.

La cybersécurité comme secteur d'exportation

Comme le régime politique canadien est largement favorable à une cybersécurité robuste, le Canada devrait commencer à imaginer un avenir où les services en matière de cybersécurité et les biens cybersécurisés deviennent des secteurs d'exportation. Le gouvernement a dans une large mesure soutenu le développement de la base de connaissances et du secteur commercial en matière de cybersécurité du Canada. Grâce à ses normes élevées, il devrait s'employer à créer des partenariats avec des entreprises et des gouvernements étrangers qui s'intéressent à une telle orientation.

25 https://ictc-ctic.ca/reports/accelerating-canadas-workforce#section-report (en anglais).

Brève incursion dans l'avenir quantique du Canada

Dans l'histoire de la technologie, surviennent parfois des bonds transformationnels qui changent complètement la donne. Si l'IA fait actuellement la une des journaux, l'essor des technologies quantiques, et notamment de l'informatique quantique, aura un effet véritablement transformationnel.

Les technologies quantiques sont basées sur la mécanique quantique, une théorie fondamentale de la physique qui décrit les propriétés physiques de la nature à l'échelle des atomes et des particules subatomiques. Les idées qui ont donné naissance au champ de la mécanique quantique sont apparues progressivement au cours des trois premières décennies du XX^{e} siècle. La mécanique quantique est l'une des théories les plus étranges, les plus impressionnantes et les moins intuitives à avoir jamais été élaborées dans l'histoire de la science. Si l'étude des atomes et des particules subatomiques peut sembler ésotérique, dans les décennies après que cette théorie eut été mise de l'avant, la connaissance de la mécanique quantique allait faciliter l'élaboration de technologies aussi diversifiées que la bombe atomique, les semi-conducteurs, les appareils d'imagerie par résonance magnétique (IRM) et les systèmes de positionnement global (GPS) qui permettent de sauver des vies.

Construire un ordinateur quantique fonctionnel est le grand rêve que caressent de nombreux scientifiques quantiques. Au fur et à mesure que progressera cette technologie, l'impact des outils et des techniques quantiques sur nos systèmes et nos méthodes de communication ne fera que s'accroître. Les méthodes de chiffrement traditionnelles reposent sur la difficulté que représentent la décomposition en produit de

facteurs premiers de grands nombres ou la résolution de problèmes de logarithme discret, deux tâches que les ordinateurs quantiques seraient en mesure de prendre en charge plus rapidement, selon un facteur exponentiel. Cela signifie qu'une fois que l'informatique quantique aura atteint un niveau de maturité suffisant, de nombreux protocoles de chiffrement existants ne seront plus sécurisés, ce qui pourrait exposer des communications, des transactions financières et des secrets d'État sensibles.

Les entreprises et les décideurs canadiens doivent se préparer à la transition menant à la cryptographie post-quantique, qui s'entend de nouvelles méthodes cryptographiques à résistance quantique. Des organisations comme le National Institute of Standards and Technology (NIST) des États-Unis s'emploient actuellement à normaliser des algorithmes cryptographiques à résistance quantique. Le Canada participe activement à ces efforts techniques. Par ailleurs, le Centre canadien pour la cybersécurité de même que des initiatives gouvernementales comme Quantum-Safe Canada investissent dans des solutions de cryptographie à résistance quantique. Ces efforts visent notamment à faire passer les systèmes informatiques du gouvernement canadien à des algorithmes post-quantiques[26].

Annoncée avec un investissement de 360 millions de dollars sur une période de sept ans dans le budget fédéral de 2021, la Stratégie quantique nationale du Canada priorise de manière explicite la cybersécurité à résistance quantique. Le rapport de la Stratégie quantique nationale du Canada[27] souligne le « risque élevé » que l'informatique quantique pose à l'égard de la cryptographie actuelle et incite vivement le gouvernement à « hausser le niveau de sensibilisation à l'égard des problèmes liés à la sécurité quantique » [Traduction], en plus d'inciter à l'adoption d'un sentiment d'urgence pour y répondre[28].

Le Canada est un leader dans le domaine de la recherche quantique, alors que des institutions comme l'Institute for Quantum Computing (IQC) de l'Université de Waterloo et que des entreprises comme Xanadu Quantum Technologies développent des mesures de sécurité à résistance quantique. Les entreprises canadiennes combinent des techniques de cryptographie traditionnelles à des techniques à résistance quantique pour assurer la protection à long terme des données. Alors que des entreprises canadiennes de matériel quantique comme Xanadu et DWave Systems continuent à progresser, elles jouent en vérité un rôle double – dans la mesure où elles renforcent l'économie, d'une part, et où elles rapprochent le jour où

26 https://www.cyber.gc.ca/fr/orientation/preparez-votre-organisation-menace-pose-informatique-quantique-itsap-00017.

27 https://ised-isde.canada.ca/site/strategie-quantique-nationale/fr/strategie-quantique-nationale-canada.

28 Demystifying Canada's Quantum Strategy | InfoSec Global) (en anglais)

les machines quantiques seront en mesure de briser le chiffrement classique, d'autre part. Cette dynamique a incité les entreprises locales de cybersécurité à créer dès aujourd'hui des solutions adaptées à la menace de demain, en réalisant des innovations dans le domaine des certificats hybrides, des outils d'évaluation des risques quantiques et des aides au déploiement de la cryptographie post-quantique[29]. Des sociétés comme Quantum Bridge Technologies se spécialisent dans les communications à résistance quantique[30].

Les organismes de réglementation financière de même que les agences de sécurité canadiens se préparent également à la transition vers la cryptographie post-quantique. Le Canada fait partie du groupe d'experts en cybersécurité du G7 (*G7 Cyber Expert Group*) qui, en 2022, formulait l'avertissement selon lequel les institutions financières devaient entreprendre de se tourner vers la cryptographie post-quantique pour protéger les données sensibles[31]. Des secteurs tels que ceux de l'énergie et des soins de santé, qui traitent des données sensibles à longue durée de vie, sont invités par le Centre canadien pour la cybersécurité à tenir compte de la menace de type « recueillir maintenant, décrypter plus tard » – menace selon laquelle les adversaires subtilisent aujourd'hui des données chiffrées en vue de les déchiffrer une fois qu'un ordinateur quantique suffisamment puissant et précis sera disponible[32].

À mesure que progresse l'informatique quantique, les entreprises et les décideurs politiques canadiens doivent prendre des mesures proactives pour s'assurer que le chiffrement demeure robuste face aux menaces de demain. Le gouvernement canadien devrait encourager l'adoption de solutions E2EE à résistance quantique dans les infrastructures essentielles ainsi qu'au niveau des finances, des soins de santé et de la sécurité nationale. En effectuant la transition menant au cryptage post-quantique et en maintenant des protections E2EE robustes, le Canada peut préserver son infrastructure numérique, protéger la vie privée des citoyens et demeurer un leader en matière de cybersécurité au niveau mondial.

29 ISARA Dedicates Four Hybrid Certificate Patents to the Public … (en anglais)

30 Quantum Bridge Gains Fast-Track Approval in Canada for Quantum-Safe Encryption with DSKE and Post-Quantum Cryptography (en anglais)

31 G7 Cyber Expert Group Warns of Quantum Computing Risks in (en anglais)

32 https://www.cyber.gc.ca/fr/orientation/preparez-votre-organisation-menace-pose-informatique-quantique-itsap-00017

Recommandations en matière de politique

Sur la base de l'analyse qui précède, le présent rapport propose au gouvernement canadien et aux parties prenantes les recommandations en matière de politique suivantes pour renforcer la protection de la vie privée, le chiffrement et la cybersécurité d'une manière qui favorise à la fois la sécurité et la prospérité économique. Ces recommandations visent à garantir que le Canada demeure un leader en matière de confiance numérique, qu'il protège ses intérêts contre les cybermenaces et qu'il favorise un écosystème technologique prospère.

Politique de chiffrement et sécurité nationale

1. S'engager publiquement à préserver un chiffrement fort et à rejeter les portes dérobées : Le gouvernement du Canada devrait publier une déclaration de principe claire et fortement médiatisée affirmant que le chiffrement fort et sans compromis demeurera légal et accessible au Canada. Il n'exigera pas des entreprises technologiques qu'elles intègrent des failles ou des portes dérobées dans leurs produits. Il n'y aura ni déchiffrement obligatoire ni « accès exceptionnel ». L'engagement du Canada en faveur d'un chiffrement fort enverrait un signal clair aux entreprises et au public canadien, consolidant la position du pays selon laquelle la sécurité et la vie privée ne seront pas sacrifiées. Cet engagement public rejetterait également les discours portant sur l'instauration d'un « équilibre » dans la politique de chiffrement. Au contraire, il indiquerait clairement qu'un chiffrement fort est la condition préalable à une gouvernance sûre, à la protection de la vie privée et à l'innovation.

2. Proclamer le chiffrement en tant qu'infrastructure essentielle : Traiter le chiffrement robuste comme un élément non négociable pour la sécurité nationale, la souveraineté numérique et la compétitivité économique mondiale du Canada. Veiller à ce que le chiffrement fort soit soutenu dans l'ensemble du pays.

Capacités en matière d'application de la loi et d'enquêtes

3. Investir dans des solutions de rechange en matière d'enquête : Il existe de nombreuses façons pour les responsables de l'application de la loi de mener des enquêtes efficaces sans pour autant imposer l'intégration de vulnérabilités dans les technologies auxquelles ont recours les Canadiens. Par exemple, le gouvernement pourrait, soit directement, soit en soutenant des entreprises canadiennes innovantes, financer des programmes de travail solides portant sur l'analyse avancée et la criminalistique ciblée qui ne compromettent pas le chiffrement. Les responsables de l'application de la loi pourraient également explorer plus avant l'apport du piratage légal. Cela ferait partie d'un programme de travail plus vaste soutenant l'innovation en matière d'accès légal. Celui-ci mettrait spécifiquement l'accent sur le financement de la recherche et du développement de méthodes d'enquête qui fonctionnent dans le respect des contraintes de chiffrement.

4. Favoriser la coopération volontaire : Encourager les cadres de collaboration entre les fournisseurs de technologies et les responsables de l'application de la loi qui protègent la vie privée des utilisateurs et l'intégrité des systèmes. De tels programmes peuvent instaurer la confiance et produire des résultats novateurs sans pour autant « dégrader l'ingénierie ».

Cybersécurité et infrastructures essentielles

5. Normaliser les exigences en matière de chiffrement fort : La normalisation des normes de chiffrement fort représente une étape essentielle. Le gouvernement fédéral devrait collaborer avec les provinces pour exiger l'E2EE et des garanties cryptographiques avancées dans les secteurs réglementés, dont la finance, les soins de santé et l'énergie.

6. Renforcer les capacités institutionnelles : Le gouvernement du Canada devrait augmenter les ressources du Centre canadien pour la cybersécurité afin qu'il dirige la mise en œuvre du chiffrement et l'adoption d'infrastructures sécurisées. Il devrait également déterminer comment il pourrait mieux collaborer avec l'organisme Canadian Cyber Threat Exchange afin de diffuser les bonnes cyberpratiques auprès des entreprises et des institutions non gouvernementales canadiennes.

7. Promouvoir le chiffrement dans la politique de sécurité nationale : Le gouvernement du Canada devrait intégrer les normes de chiffrement dans ses stratégies en matière de marchés publics et de résilience numérique. En agissant de la sorte, il aurait directement recours à des technologies sécurisées et robustes ou contribuerait à leur diffusion.

8. Aider les entreprises – notamment les PME – à améliorer leurs défenses en matière de cybersécurité : De nombreuses atteintes et plusieurs incidents liés aux rançongiciels tirent parti du fait que les petites entreprises disposent de moins de ressources et d'expertise pour déployer des défenses solides. Le gouvernement devrait étendre les programmes qui offrent des incitations financières et une expertise pour les mises à niveau de cybersécurité. Il pourrait notamment s'agir de crédits d'impôt pour les investissements certifiés en matière de cybersécurité (p. ex., adoption de l'authentification multifactorielle, chiffrement des données au repos, formation du personnel à la sécurité), ou de subventions/coupons pour permettre aux PME d'obtenir des évaluations et des améliorations en matière de cybersécurité. L'extension du programme de certification en cybersécurité CyberSécuritaire Canada est une étape pratique. Il y aurait lieu de le faire connaître et peut-être même d'offrir une modeste subvention pour le coût de la certification aux personnes qui y participent pour la première fois. Le gouvernement pourrait également envisager de créer une « place de marché de la cybersécurité » où des fournisseurs canadiens agréés proposeraient des remises ou des formules spéciales pour les besoins des petites entreprises (antivirus, sauvegardes gérées, etc.). En améliorant la sécurité de base de toutes les entreprises, le Canada réduit la surface d'exposition globale.

9. Améliorer la cyberculture et le perfectionnement de la main-d'œuvre : Une position enviable à long terme en matière de cybersécurité et de protection de la vie privée passe par un public averti et une main-d'œuvre qualifiée. Le gouvernement devrait étendre les programmes d'alphabétisation numérique de manière à y inclure une formation de base à la cybersécurité et à la protection de la vie privée à l'intention des citoyens. Par exemple, pourraient être inclus des modules portant sur des sujets tels que l'utilisation des outils de chiffrement et la manière d'éviter l'hameçonnage. En parallèle, le gouvernement devrait multiplier les initiatives visant à combler le manque de talents en cybersécurité. Il pourrait notamment offrir des bourses aux étudiants en cybersécurité, inciter les professionnels en milieu de carrière à suivre une formation en cybersécurité et accélérer l'immigration d'experts en cybersécurité en provenance de l'étranger.

Cryptographie post-quantique (CPQ)

10. Mener la transition vers la CPQ : S'appuyant sur ses investissements importants envers la science quantique au fil des ans, le Canada devrait imposer l'adoption rapide des normes cryptographiques post-quantiques et faire en sorte que les systèmes fédéraux respectent les recommandations du NIST. Il devrait également intégrer la CPQ dans les programmes de modernisation technologique. Il doit veiller à ce que les efforts de transformation numérique dans l'ensemble du gouvernement incluent des mises à niveau de chiffrement ou de cryptage à résistance quantique. Enfin, en ce qui concerne la main-d'œuvre, le Canada devrait investir conjointement avec les universités et les entreprises dans la formation des professionnels à la cryptographie quantique, à la modélisation des risques et aux communications sécurisées.

Diversification des échanges

11. Intégrer la cybersécurité et la protection de la vie privée à la stratégie économique : Le Canada doit adopter sans réserve une stratégie commerciale fondée sur un niveau élevé de protection de la vie privée, de sécurité et de confiance. La qualité de ses normes et de ses pratiques devrait être au cœur de la marque canadienne dans le domaine numérique. Sur le plan opérationnel, le gouvernement du Canada pourrait lancer une initiative qui offrirait des financements et des incitations aux entreprises technologiques qui conçoivent des produits améliorant la sécurité et la protection de la vie privée, tels que des logiciels de chiffrement, une IA respectueuse de la vie privée, des plateformes de messagerie sécurisées et d'autres innovations numériques soutenant ces objectifs.

12. Gérer avec soin les enjeux numériques dans le nouvel accord commercial nord-américain : Alors que le Canada et les États-Unis poursuivent la négociation d'un nouvel accord commercial, des enjeux fondamentaux de politique numérique pourraient bien figurer à l'ordre du jour. Le Canada devra faire preuve de fermeté pour veiller à ce que la protection de la vie privée et d'autres droits fondamentaux ne soient pas mis en péril.

Engagement international

13. Promouvoir des normes mondiales solides en matière de chiffrement : En se dotant d'une politique de chiffrement forte, le Canada est incité à façonner une politique de chiffrement à l'échelle internationale. L'un des moyens d'y parvenir consiste à renforcer le leadership du Canada au sein de l'Internet Engineering Task Force (IETF), de l'Organisation internationale de normalisation (ISO) et des forums multilatéraux sur la cybersécurité afin d'élaborer des normes de chiffrement résilientes. Le Canada devrait également prioriser ses efforts en matière de chiffrement sur le plan diplomatique. Il s'agit notamment de s'opposer aux efforts internationaux visant à affaiblir le chiffrement dans les accords sur le commerce numérique ou les accords de surveillance transfrontalière.

14. Favoriser les alliances internationales sur la protection de la vie privée et les normes de cybersécurité au-delà du Groupe des cinq : Le Canada devrait tirer parti de sa position unique pour créer des coalitions plus larges sur la politique numérique – par exemple, en travaillant de concert avec l'Union européenne, le Japon et d'autres démocraties sur une déclaration commune ou un cadre qui approuve des écosystèmes de chiffrement solides et sécurisés au plan conceptuel. Ce faisant, le Canada fait valoir qu'il représente un « maillon fort » du mouvement de la cybersécurité. En agissant de la sorte, le Canada peut efficacement rejeter les critiques de ses partenaires du Groupe des cinq.

Consultations et analyses continues

15. Revoir et mettre continuellement à jour les politiques en tenant compte de l'avis des parties prenantes : Les technologies et les menaces évoluent rapidement. Le gouvernement devrait implanter un cycle de révision régulier, tous les trois ans, des politiques majeures comme celles qui portent sur la cybersécurité et la protection de la vie privée. En institutionnalisant les processus de révision, le Canada peut demeurer agile et éviter que ses politiques ne stagnent.

Pour conclure

Le Canada traverse une période de changements importants et s'inquiète de son avenir. Le nouveau gouvernement doit faire preuve d'audace et de clarté.

En mettant en œuvre les présentes recommandations, le Canada peut renforcer simultanément son économie et sa sécurité. Le principe directeur est le suivant : la protection de la vie privée, le chiffrement et la cybersécurité ne sont pas des obstacles à surmonter, mais plutôt des assises sur lesquelles construire. En veillant à ce que nos lois et nos programmes rendent compte de ce principe, le Canada restera sûr, concurrentiel et libre à l'ère numérique.

Annexe 1 : bref aperçu de la protection de la vie privée au Canada

Pendant la majeure partie des 100 premières années de la Confédération, le concept de protection de la vie privée intéressait les citoyens vivant dans les villes et les villages voisins.

La protection de la vie privée commença à préoccuper les gouvernements dans les années 1960. Lors d'un débat portant sur la décriminalisation de l'homosexualité, Pierre Trudeau, alors ministre de la Justice, déclara en 1967 que « l'État n'a pas sa place dans les chambres à coucher de la nation ». Il s'agissait, en substance, d'une déclaration portant sur ce que le gouvernement n'inclurait pas dans le *Code criminel*. Dans les années 1970, les gouvernements fédéral et provinciaux commencèrent à promulguer des lois destinées à protéger spécifiquement la vie privée des citoyens et à garantir l'accès aux informations gouvernementales. Dans les années 1990, de nouveaux défis allaient résulter de l'essor d'Internet et des technologies numériques.

Les lois canadiennes sur la protection de la vie privée et des données influencent fortement l'utilisation du chiffrement comme mesure de protection des renseignements personnels, ce qui fait du chiffrement une pratique exemplaire pour protéger la confidentialité des données. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) de 2000, la loi fédérale qui régit le secteur privé, exige des organisations qu'elles protègent les renseignements personnels par des mesures de sécurité appropriées. Le septième principe (4.7) stipule explicitement que les mesures de protection devraient comprendre des mesures techniques, par exemple, l'usage de mots de passe et du chiffrement. Ce principe crée une attente juridique selon laquelle les entreprises auront recours au chiffrement, entre autres contrôles, pour empêcher l'accès non autorisé aux renseignements personnels. Le Commissariat à la protection de la vie privée du Canada (CPVP) a renforcé ce principe dans ses lignes directrices, en encourageant les entreprises à chiffrer les données sensibles stockées sur les ordinateurs portables et les supports mobiles dans le cadre de la prévention des atteintes à la vie privée.

Les lois provinciales sur la protection de la vie privée dans le secteur privé (comme la loi sur la protection des renseignements personnels de l'Alberta et de la Colombie-Britannique de même que la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec) reflètent les exigences fédérales, en demandant aux organisations d'utiliser des mesures de sécurité raisonnables – souvent satisfaites par le recours à un chiffrement fort pour les données sensibles.

Dans le secteur public, la *Loi sur la protection des renseignements personnels* (1985) fédérale et les lois provinciales similaires obligent les institutions gouvernementales à protéger les renseignements personnels qu'elles détiennent. Bien que ces lois n'énumèrent pas de technologies spécifiques, dans la pratique, le chiffrement est la pierre angulaire de la politique de sécurité informatique du gouvernement pour la protection des données sensibles et personnelles. Par exemple, les directives du gouvernement fédéral, qui cadrent avec les normes du Centre de la sécurité des télécommunications Canada, imposent le chiffrement pour la transmission et le stockage des renseignements protégés. Dans le secteur de la santé, certaines lois et directives vont plus loin dans la spécification du chiffrement : la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario exige que les responsables de la santé prennent des mesures raisonnables pour sécuriser les données des patients. Le Commissaire à l'information et à la protection de la vie privée de l'Ontario a clairement indiqué que cela signifie que les informations de santé stockées sur des appareils mobiles doivent être chiffrées pour éviter les violations. Le cadre canadien de protection de la vie privée ne se contente pas d'autoriser le chiffrement, il l'encourage, voire l'exige, en tant que meilleure pratique pour se conformer aux obligations juridiques en matière de protection de la confidentialité.

Chambre de Commerce du Canada | Canadian Chamber of Commerce

Centre de l'avenir des affaires de la Chambre de Commerce du Canada | Canadian Chamber Future of Business Centre