Connexions vulnérables

Le comité d'experts sur la sécurité publique à l'ère du numérique

CCA | CAC

Connexions vulnérables

Le comité d'experts sur la sécurité publique à l'ère du numérique

CONSEIL DES ACADÉMIES CANADIENNES
180 rue Elgin, bureau 1401, Ottawa (Ontario) Canada K2P 2K3

Le projet sur lequel porte ce rapport a été entrepris avec l'approbation du conseil d'administration du Conseil des académies canadiennes (CAC). Les membres du conseil d'administration sont issus de la Société royale du Canada (SRC), de l'Académie canadienne du génie (ACG) et de l'Académie canadienne des sciences de la santé (ACSS), ainsi que du grand public. Les membres du comité d'experts responsables du rapport ont été choisis par le CAC en raison de leurs compétences particulières et dans le but d'obtenir un éventail équilibré de points de vue.

Ce rapport a été rédigé à l'intention Sécurité publique Canada (SP), qui souhaitait obtenir une évaluation indépendante. SP n'a aucunement pris part à la sélection des membres du comité d'experts ni à la rédaction du rapport. Les opinions, constatations et conclusions présentées dans cette publication sont celles des auteurs, soit les membres du comité d'experts sur la sécurité publique à l'ère du numérique, et ne reflètent pas nécessairement le point de vue des organisations auxquelles ils sont affiliés ou dans lesquelles ils travaillent.

Bibliothèque et Archives Canada

ISBN : 978-1-990592-24-9 (livre)
978-1-990592-25-6 (livre électronique)

Ce rapport doit être cité de la façon suivante :

CAC — Conseil des académies canadiennes, 2023. *Connexions vulnérables*. Ottawa, ON, Le comité d'experts sur la sécurité publique à l'ère du numérique, CAC.

Avis de non-responsabilité

Les données et l'information Internet mentionnées dans le présent rapport étaient exactes, à la connaissance du CAC, au moment de la publication. En raison de la nature dynamique d'Internet, des ressources gratuites et accessibles au public peuvent subséquemment faire l'objet de restrictions ou de frais d'accès, et l'emplacement des éléments d'information peut changer lorsque les menus et les pages Web sont modifiés.

Ce projet a été rendu possible grâce au soutien du gouvernement du Canada

Le comité d'experts sur la sécurité publique à l'ère du numérique aimerait remercier les Inuits, les Métis et les Premières Nations d'avoir, depuis toujours, assuré l'intendance du territoire qu'on appelle aujourd'hui le Canada.

Le Conseil des académies canadiennes (CAC) reconnaît que ses bureaux d'Ottawa sont situés sur le territoire ancestral non cédé et non abandonné de la Nation algonquine Anishinaabe, qui a pris soin de l'environnement de ce territoire depuis des millénaires. Bien que les bureaux du CAC se trouvent à cet endroit, ses travaux en faveur de la prise de décision éclairée par des données probantes peuvent avoir des bienfaits plus étendus dans tout le Canada. Le CAC reconnaît l'importance de s'appuyer sur un large éventail de connaissances et d'expériences pour élaborer des politiques qui permettront de bâtir une société plus forte, plus équitable et plus juste.

Le Conseil des académies canadiennes

Le CAC est un organisme sans but lucratif qui réalise des évaluations indépendantes fondées sur les données probantes, par l'entremise de comités d'experts, afin de guider l'élaboration de politiques publiques au Canada. Dirigés par un conseil d'administration et guidés par un comité consultatif scientifique, les travaux du CAC répondent à une définition large de la science, qui intègre les sciences naturelles, sociales et de la santé, ainsi que le génie et les sciences humaines. Les évaluations du CAC sont réalisées par des comités multidisciplinaires et indépendants d'experts canadiens et étrangers. Ces évaluations cherchent à cerner les problèmes nouveaux, les lacunes de connaissances, les forces du Canada, et les tendances et pratiques internationales. Ces études fournissent aux décideurs gouvernementaux, aux chercheurs et aux parties prenantes l'information de grande qualité dont ils ont besoin pour élaborer des politiques publiques éclairées et innovatrices.

Tous les rapports d'évaluation du CAC sont soumis à un examen formel et sont publiés et mis à la disposition du public sans frais. Les évaluations peuvent être entreprises à la demande de fondations, d'organismes non gouvernementaux, du secteur privé ou de tout ordre de gouvernement.

www.rapports-cac.ca

@cca_reports

Les académies

Le CAC est soutenu par ses trois académies fondatrices :

La Société royale du Canada (SRC)

Fondée en 1882, la SRC comprend l'Académie des arts, des lettres et des sciences, ainsi que le tout premier organisme canadien de reconnaissance multidisciplinaire destiné à la nouvelle génération d'intellectuels canadiens : le Collège de nouveaux chercheurs et créateurs en art et en science. Sa mission consiste à reconnaître les plus éminents intellectuels, chercheurs et créateurs, à conseiller les gouvernements et les organisations, et à favoriser l'avancement du savoir et de l'innovation au Canada et avec d'autres académies nationales partout dans le monde.

L'Académie canadienne du génie (ACG)

L'ACG est l'organisme national par l'entremise duquel les ingénieurs les plus chevronnés et émérites du Canada offrent des conseils stratégiques sur des enjeux d'importance primordiale pour le pays. L'ACG est un organisme indépendant, autonome et à but non lucratif qui a été fondé en 1987. Les Fellows de l'ACG sont nommés et élus par leurs pairs, en fonction de leurs réalisations exceptionnelles et de leurs longs états de service au sein de la profession d'ingénieur. Les Fellows de l'ACG s'engagent à faire en sorte que l'expertise du Canada en ingénierie soit mise à contribution pour le plus grand bien de tous les Canadiens et de toutes les Canadiennes.

L'Académie canadienne des sciences de la santé (ACSS)

L'ACSS reconnaît l'excellence dans les sciences de la santé en nommant ses membres en fonction de leurs réalisations exceptionnelles dans les disciplines universitaires des sciences de la santé au Canada et de leur volonté de servir le public canadien. L'ACSS fournit des évaluations opportunes, factuelles et impartiales sur des sujets qui touchent la santé de la population canadienne, et recommande des solutions stratégiques et réalisables. Fondée en 2004, l'ACSS nomme de nouveaux membres sur une base annuelle. L'ACSS est dirigée par un conseil d'administration constitué de volontaires et par un comité de direction.

Comité d'experts sur la sécurité publique à l'ère du numérique

Guidé par son comité consultatif scientifique, son conseil d'administration et ses académies fondatrices, le CAC a constitué le **comité d'experts sur la sécurité publique à l'ère du numérique** pour mener à bien ce projet. Chacun des membres de ce comité a été choisi pour son expertise, son expérience et son leadership éprouvé dans des domaines pertinents pour le projet.

Jennifer Stoddart, O.C., C.Q., Ad.E. (présidente), avocate, conseillère stratégique, Fasken; ancienne commissaire à la protection de la vie privée du Canada (Montréal, Qc)

Benoît Dupont, professeur, École de criminologie, Chaire de recherche du Canada en cybersécurité, Chaire de recherche en prévention de la cybercriminalité, Université de Montréal; directeur scientifique, Réseau intégré sur la cybersécurité (Montréal, Qc)

Richard Frank, professeur agrégé, École de criminologie, directeur du Centre international de recherche sur le cybercrime, Université Simon Fraser (Burnaby, C.-B.)

Colin Gavaghan, professeur, Institut des futurs numériques de Bristol et École de droit, Université de Bristol (Bristol, Royaume-Uni)

Laura Huey, professeure, Département de sociologie, Université Western (London, Ont.)

Emily Laidlaw, Chaire de recherche du Canada en droit de la cybersécurité et professeure agrégée, Faculté de droit, Université de Calgary (Calgary, Alb.)

Arash Habibi Lashkari, professeur agrégé et Chaire de recherche du Canada en cybersécurité, École des technologies de l'information, Université York (Toronto, Ont.)

Christian Leuprecht, professeur distingué en leadership de la promotion de 1965, Département de science politique et d'économie, Collège militaire royal du Canada directeur, Institut des relations intergouvernementales, École d'études politiques, Université Queen's (Kingston, Ont.)

Florian Martin-Bariteau, professeur agrégé de droit et Chaire de recherche en technologie et société, Université d'Ottawa; Fellow, Centre d'études sur Internet et la société Berkman-Klein, Université Harvard (Ottawa, Ont.)

Shannon Parker, directrice, Conseils en matière de stratégie et de risque cyberfacilités, Deloitte Canada (Saskatoon, Sask.)

Christopher Parsons, conseiller principal en matière de technologie et de politiques, Commissaire à l'information et à la protection de la vie privée de l'Ontario. Anciennement, associé de recherche principal et administrateur délégué, Telecom Transparency Project du Citizen Lab, École d'affaires mondiales et de politique publique Munk, Université de Toronto (Toronto, Ont.)

Jad Saliba, fondateur et directeur de la technologie, Magnet Forensics (Waterloo, Ont.)

Heidi Tworek, chaire de recherche du Canada et directrice, Centre d'études sur les institutions démocratiques; professeure agrégée, École des politiques publiques et des affaires mondiales et Département d'histoire, Université de la Colombie-Britannique (Vancouver, C.-B.)

Message du président-directeur général

La technologie change fondamentalement la façon dont nous vivons, travaillons et interagissons en ligne. Naviguer dans l'environnement numérique — de la protection d'une multitude de mots de passe à la vigilance face aux escroqueries — peut s'avérer complexe dans le meilleur des cas. Pour les personnes qui se retrouvent la cible d'acteurs malveillants, les répercussions peuvent être particulièrement lourdes. Les conséquences de la cyberfraude, du harcèlement et des abus, ainsi que d'autres méfaits en ligne, sont importantes et peuvent profondément changer la vie. Au Canada, et partout dans le monde, ces types d'actes sont en hausse.

Lorsqu'une personne devient la cible d'un méfait cyberfacilité, déterminer ses recours et comment en bénéficier peut présenter une série d'obstacles. Le droit criminel canadien qui s'applique à la cybercriminalité a été conçu à l'origine pour les actes commis hors ligne et peut ne pas s'appliquer aussi directement. Les forces de l'ordre sont aux prises avec des lacunes en matière de formation, des limites dans les données et des problèmes de ressources. Pendant ce temps, les auteurs de ces actes utilisent souvent l'anonymat, le chiffrement et la rapidité de l'évolution technologique à leur avantage.

Pour compliquer encore les choses, tous les préjudices en ligne ne sont pas le résultat d'un comportement illégal; ils se situent sur un spectre de légalité et de criminalité. C'est par exemple le cas de la mésinformation sur Internet et de certaines formes de discours haineux, qui peuvent repousser les limites socialement acceptées d'un comportement éthiquement approprié, sans pour autant franchir le seuil de l'illégalité. Voilà pourquoi une réforme législative ne suffira pas à résoudre les problèmes posés par la croissance et l'utilisation nuisible des technologies de l'information et des communications (TIC). Au contraire, toutes les facettes de la société auront un rôle à jouer dans la lutte contre les cybercrimes et les cyberméfaits.

Reconnaissant les changements et les défis que les TIC ont introduits dans l'espace public numérique, Sécurité publique Canada a demandé au CAC d'examiner les pratiques exemplaires qui pourraient réduire les risques pour la sécurité publique tout en respectant les droits de la personne et la vie privée.

Connexions vulnérables se penche sur les menaces en constante évolution qui pèsent sur l'environnement numérique. Ce rapport examine les problèmes et les possibilités en matière de réglementation, de prévention, d'enquête, de poursuites et de lutte contre les crimes et les méfaits facilités par la technologie, et décrit diverses approches réglementaires canadiennes et étrangères.

Au nom du CAC, j'aimerais remercier le comité d'experts pour la qualité de son travail dans ce rapport, qui a été éclairé par leur expertise approfondie en cybersécurité, en histoire, en criminologie, en forces de l'ordre et en droit et gouvernance. Sa présidente, Jennifer Stoddart, a habilement dirigé le comité tout au long d'un processus mené à la fois virtuellement et en personne. Comme toujours, les conseils et la supervision fournis par le conseil d'administration et le comité consultatif scientifique du CAC tout long de l'évaluation ont été extrêmement précieux.

Eric M. Meslin, Ph. D., MSRC, MACSS
Président-directeur général, Conseil des académies canadiennes

Message de la présidente

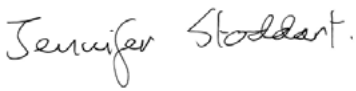
Les technologies de l'information et des communications ont eu un impact profond sur la vie quotidienne et nos univers numérique et physique sont désormais pratiquement indissociables. Ces dernières décennies, les technologies numériques sont devenues essentielles pour obtenir des soins de santé et une éducation, accéder aux services publics, participer à la vie active, entretenir des liens sociaux, etc. Si ces technologies ont apporté des avantages non négligeables, leur omniprésence signifie également que tout le monde, même les personnes hors ligne, peut devenir la cible de crimes ou de comportements préjudiciables cyberfacilités. En outre, la prolifération des outils technologiques numériques a eu des conséquences considérables sur la vie privée, composante essentielle de la sécurité personnelle et de la dignité.

Les actes cyberfacilités préjudiciables sont en hausse au Canada et provoquent des dommages physiques, économiques, psychologiques et de réputation importants pour ses habitants. Cependant, les structures de sécurité publique actuelles et les approches suivies par le secteur privé ne se sont pas convenablement adaptées à une situation radicalement modifiée par les technologies numériques. Les gouvernements au Canada cherchent donc à rattraper le temps perdu en s'efforçant d'améliorer la sécurité de l'écosystème numérique, tout en protégeant les droits et libertés constitutionnels. Dans le même temps, le système judiciaire est confronté à des difficultés de taille pour appliquer les cadres juridiques existants qui interdisent certains comportements préjudiciables sur Internet. La police est souvent entravée dans sa capacité à enquêter sur ces activités criminelles.

Connexions vulnérables examine la manière dont les activités préjudiciables et illégales ont évolué sous l'effet des technologies numériques, les problèmes qui en découlent pour les décideurs et les forces de l'ordre, ainsi que les possibilités de réglementation, de prévention et d'enquête concernant les préjudices cyberfacilités. Il illustre à la fois la complexité et l'urgence de ces questions et montre que la promotion d'un écosystème numérique plus sûr ne peut relever des actions d'un seul organisme public, qu'il soit provincial, fédéral ou étranger. La coopération et la coordination entre États sont essentielles, car les préjudices cyberfacilités traversent les frontières et continuent d'évoluer rapidement. En outre, les solutions ne se trouvent pas uniquement entre les mains des gouvernements; le secteur privé, y compris les platesformes de médias sociaux, a un rôle essentiel à jouer, tout comme la société civile.

Mes collègues membres du comité d'experts ont apporté un large éventail d'expériences et de connaissances, et je tiens à les remercier pour leur travail acharné et leur dévouement de tous les instants dans cet important projet. À mon

avis, leurs discussions et débats rigoureux ont mené à un rapport complet et stimulant. Je tiens également à remercier le personnel du CAC pour son soutien critique et sa réactivité tout au long du processus. Enfin, au nom du comité d'experts, j'aimerais remercier Sécurité publique Canada et les sept ministères et organismes fédéraux qui l'appuient* d'avoir parrainé cette évaluation et soumis cette question opportune et cruciale.



Jennifer Stoddart, O.C., C.Q., Ad.E.
Présidente du comité d'experts sur la sécurité publique à l'ère du numérique

*Patrimoine canadien; Centre de la sécurité des télécommunications Canada; Affaires mondiales Canada; Innovation, Sciences et Développement économique Canada; Justice Canada; Bureau du Conseil privé; Gendarmerie royale du Canada

Équipe de projet du Conseil des académies canadiennes

Équipe d'évaluation :	**Becky Chapman,** directrice de projet
	Adam Fortais, chercheur
	Teresa Iacobelli, associée de recherche
	Anastasia Konina, associée de recherche
	Ricardo Pelai, associé de recherche
	Kate Hemstreet, coordinatrice de projet
	Jenn Snider Cruise, coordinatrice de projet
	Tijs Creutzberg, directeur des évaluations
Avec la participation de :	
Révision	Jody Cooper
Mise en page	gordongroup
Traducteur, En-Fr	François Abraham

Examen du rapport

Le présent rapport a été examiné par les personnes répertoriées ci-dessous, qui ont été sélectionnées par le CAC pour la diversité de leurs points de vue et de leurs domaines d'expertise.

Les examinateurs ont évalué l'objectivité et la qualité du rapport. Le comité a étudié intégralement leurs observations confidentielles et a intégré bon nombre de leurs suggestions. Le CAC ne leur a pas demandé de cautionner les conclusions du rapport et ils n'ont pas vu la version finale avant publication. La responsabilité du contenu final de ce rapport incombe entièrement au comité d'experts qui l'a rédigé et au CAC.

Le CAC tient à remercier les personnes suivantes pour leur examen du présent rapport :

Aengus Bridgman, candidat au doctorat en science politique, Université McGill; ancien directeur de l'Observatoire de l'écosystème médiatique, partie du Centre d'études sur les médias, la technologie et la démocratie (Montréal, Qc)

Aurélie Campana, professeure, Département de science politique, Université Laval; ancienne titulaire de la Chaire de recherche du Canada sur les conflits et le terrorisme (2007–2017) et membre exécutive du Réseau canadien de recherche sur le terrorisme, la sécurité et la société (2015–2022) (Québec, Qc)

Ritesh Kotak, stratège numérique et en cybersécurité et cofondateur, jusTech; membre du E-Crime Cyber Council, Association canadienne des chefs de police; président du conseil consultatif des anciens étudiants du doyen sur la technologie, Faculté de droit, Université d'Ottawa (Toronto, Ont.)

Vivek Krishnamurthy, professeur de droit Samuelson-Glushko et directeur, Clinique canadienne de politiques Internet et de politiques d'intérêt public Samuelson-Glushko, Université d'Ottawa; associé au corps professoral, Centre Berkman Klein pour Internet et la société, Université Harvard; associé principal (non résident), Centre d'études stratégiques et internationales (Ottawa, Ont.)

Jacques Marcoux, directeur de la recherche et des analyses, Centre canadien de protection de l'enfance; ancien journaliste de données et journaliste d'enquête, CBC News (Winnipeg, Man.)

Brenda McPhail, directrice, Programme de protection de la vie privée, de technologie et de surveillance, Association canadienne des libertés civiles (Toronto, Ont.)

Steven Penney, professeur, Faculté de droit, Université de l'Alberta; président, Conseil consultatif du Centre d'études constitutionnelles, conseil consultatif de l'Alberta Law Review (Edmonton, Alb.)

Tamara A. Small, professeure, département de science politique, Université de Guelph (Guelph, Ont.)

Thorsten Wetzling, chef de la recherche, Unité des droits, de la surveillance et de la démocratie numériques, Stiftung Neue Verantwortung e.V. (Berlin, Allemagne)

L'examen par les pairs a été supervisé, au nom du conseil d'administration et du comité consultatif scientifique du CAC, par **Neena L. Chappell, CM, MSRC, MACSS,** professeure émérite, Institut sur le vieillissement et la santé tout au long de la vie et Département de sociologie, Université de Victoria. Son rôle était de veiller à ce que le comité d'experts prenne en considération de façon entière et équitable les avis des examinateurs. Le conseil d'administration du CAC n'autorise la publication d'un rapport de comité d'experts qu'une fois que la personne chargée de superviser l'examen du rapport par les pairs a confirmé que celui-ci satisfait bien aux exigences du CAC. Le CAC remercie madame Chappell d'avoir supervisé consciencieusement l'examen du rapport.

Résumé

Les technologies et les platesformes numériques — y compris les téléphones intelligents, les médias sociaux et d'autres applications en ligne — ont radicalement modifié la vie quotidienne au Canada, apportant des avantages considérables, mais créant aussi des risques de préjudices notables. L'expérience de chacun est façonnée d'une manière ou d'une autre par les technologies numériques, qu'elles soient virtuelles ou non. Les technologies numériques imprègnent toutes les institutions et, par conséquent, tout le monde au Canada sont de plus en plus exposés à un large éventail de menaces en ligne pour leur sécurité publique. Certaines des menaces facilitées par les technologies de l'information et des communications (TIC) ne sont pas nouvelles, mais elles se produisent désormais dans des espaces numériques et à plus grande échelle, tandis que d'autres méfaits sont nouveaux et évoluent rapidement. Dans ce contexte, le rôle des forces de l'ordre et des gouvernements dans la protection de la sécurité publique numérique est en pleine mutation et l'on ne sait pas très bien où, comment et auprès de qui chercher de l'aide lorsqu'on subit un préjudice cyberfacilité (*cyber-enabled).*

Toutes les personnes vivant au Canada sont numériques par défaut, même si elles sont hors ligne ou utilisent rarement les technologies numériques. Si ces technologies apportent des avantages considérables, elles peuvent aussi compromettre la sécurité de tous.

Reconnaissant l'importance de comprendre et de relever les défis que les TIC posent à la sécurité publique numérique, Sécurité publique Canada (ci-après « le commanditaire ») a demandé au Conseil des académies canadiennes (CAC) de constituer un comité d'experts chargé d'examiner les pratiques exemplaires qui pourraient contribuer à réduire les risques pour la sécurité publique tout en respectant les droits de la personne et la vie privée. Pour répondre à cette demande, le CAC a réuni un comité multidisciplinaire de 13 experts possédant de l'expérience et une expertise en cybersécurité, en histoire, en criminologie, en forces de l'ordre et en droit et gouvernance.

Conformément aux intérêts du commanditaire, le comité d'experts sur la sécurité publique à l'ère du numérique a focalisé ses recherches et ses analyses sur les actes qui utilisent la technologie comme instrument *(cyberfacilités*) pour infliger des préjudices aux gens[1]. Il s'agit notamment de la radicalisation, des

abus en ligne et de la cyberfraude, qui se déroulent sur un spectre de légalité et de criminalité. Si les activités qui font l'objet du présent rapport sont préjudiciables, la ligne de démarcation entre comportement licite et comportement illicite n'est pas toujours claire, et il n'y a pas non plus de consensus sur l'endroit où cette ligne devrait se situer.

Réponse aux questions du mandat

Comment les activités criminelles graves (notamment le crime organisé et l'exploitation sexuelle des enfants) et causant des préjudices en ligne (notamment la désinformation, l'utilisation d'Internet à des fins extrémistes violentes et terroristes) au Canada ont-elles évolué pour exploiter le paysage changeant des technologies de l'information et des communications (TIC)?

Les crimes cyberfacilités sont largement sous-déclarés, mais les données dont on dispose montrent que la fréquence de leur déclaration par la police, ainsi que le nombre d'auteurs de cybermenaces, est en augmentation au Canada. Il est important de noter que la prolifération des cybercrimes n'est pas seulement le résultat de l'utilisation accrue des technologies numériques, mais qu'elle peut être aussi liée à des facteurs sociaux et économiques, tels que la polarisation, l'isolement et la privation de droits économiques et politiques.

1 Les actes préjudiciables cyberdépendants (p. ex. l'utilisation de logiciels malveillants) n'entrent pas dans le cadre du présent rapport, mais sont abordés dans les cas où les données probantes sont intéressantes pour les préjudices cyberfacilités.

Les technologies ont radicalement modifié la vie quotidienne au Canada, mais les approches adoptées par les gouvernements et le secteur privé, notamment les lois et les politiques, n'ont pas toujours suivi le rythme des nouveaux défis.

De nombreux éléments montrent comment il est possible d'exploiter les TIC pour commettre un large éventail d'actes préjudiciables, licites ou illicites, qui ont de graves répercussions physiques, psychologiques et financières. Par exemple, les platesformes numériques ont été utilisées pour faciliter la traite des femmes et des enfants en permettant aux auteurs de recruter, de faire de la publicité et de communiquer plus facilement; le harcèlement et les abus en ligne sont de plus en plus fréquents sur les grandes platesformes de médias sociaux, ils entraînent des dommages physiques et psychologiques et ont un effet paralysant sur la liberté d'expression des victimes et des survivants. Les TIC facilitent à la fois les activités frauduleuses (p. ex. utilisation des médias sociaux pour trouver des victimes potentielles et communiquer avec elles) et permettent des tactiques de fraude plus perfectionnées, comme l'usurpation d'adresse et l'hameçonnage, qui sont difficiles à détecter. La rapide prolifération de la mésinformation en ligne a encore exacerbé la cyberfraude et la propagation de la haine.

L'anonymat est l'un des principaux éléments qui permettent une utilisation préjudiciable des technologies numériques. Par exemple, le grand anonymat des utilisateurs dans les plateformes d'échanges de cryptomonnaies, sur le Web clandestin (*Dark Web*) et sur les réseaux privés virtuels permet aux acteurs malveillants de dissimuler leur identité ainsi que leurs activités illégales ou nuisibles. Les technologies numériques ont également rendu possibles de nouveaux mécanismes de financement des activités criminelles; les cryptomonnaies, par exemple, posent des problèmes aux forces de l'ordre, car elles peuvent être utilisées pour financer des crimes d'un État à un autre, pour payer des biens ou des services illégaux et pour blanchir de l'argent.

Quels défis les progrès des TIC (notamment le chiffrement et la 5G) posent-ils pour la prévention, la lutte, les enquêtes et les poursuites relatives aux crimes et pour l'atténuation des préjudices en ligne?

Un élément crucial de la prévention des méfaits cyberfacilités est de disposer de données sur le lieu et la fréquence de ces méfaits, ainsi que sur leurs effets sur les victimes et les survivants. Dans le domaine des actes criminels, les rapports de police sont des sources de données importantes qui donnent une certaine idée de ces actes, mais une multitude de facteurs limite l'utilité de ces données. Les

crimes cyberfacilités ne sont pas signalés de manière cohérente d'un territoire policier à l'autre, en partie à cause des contraintes de capacité des unités de police, ce qui entraîne de gros écarts dans les chiffres entre les municipalités. Il en résulte que les données sur les cybercrimes sont extrêmement limitées au Canada, tout comme les recherches et les données sur les autres méfaits. En outre, la recherche sur les pratiques de cybersécurité et forces de l'ordre en général est également insuffisante. Ces lacunes dans les données entravent la capacité des forces de l'ordre et des différents ordres de gouvernement à diriger les ressources, à évaluer la pertinence et le potentiel des nouvelles approches et à déterminer l'efficacité des mesures instaurées.

Le volume des données, la limitation des ressources et les lacunes de compétences, ainsi que la désuétude des structures organisationnelles et les progrès technologiques, compliquent le travail des forces de l'ordre quand il s'agit de prévenir les crimes cyberfacilités, d'enquêter, d'analyser les faits et d'intenter des poursuites.

La rapidité des progrès technologiques complique l'application, l'interprétation et l'exécution des lois. Chaque technologie émergente (p. ex. la 5G, le chiffrement de bout en bout) crée ses propres difficultés, qui justifieraient un rapport complet; cependant, il existe également des écueils communs transversaux. Un problème fondamental est que le droit criminel canadien qui s'applique aux crimes cyberfacilités a été conçu pour des actes hors ligne. Lorsque de nouvelles technologies numériques sont lancées sur le marché, généralement avec peu ou pas de surveillance ou de préparation réglementaire, elles peuvent avoir de graves répercussions sur la sécurité publique et sur la vie privée. En raison de la rapidité de l'innovation contemporaine en matière de TIC, les forces de l'ordre, les décideurs et les utilisateurs de TIC sont régulièrement contraints de réagir aux nouveaux modes de perpétration des crimes. De plus, l'absence d'orientation et de surveillance de l'utilisation des nouvelles technologies par les forces de l'ordre peut mener à des occasions manquées ou à un emploi répréhensible des outils, qui viole la vie privée ou d'autres droits.

La question de la compétence territoriale constitue un obstacle de taille à la lutte contre les préjudices cyberfacilités. Les auteurs de cybermenaces peuvent se trouver physiquement n'importe où dans le monde et, souvent, la victime et l'auteur ne sont pas situés dans le même pays. Étant donné le grand anonymat et les multiples couches de chiffrement que certaines platesformes numériques offrent aux utilisateurs, il peut être difficile de recueillir des preuves pertinentes, notamment l'origine d'un acte criminel particulier. Par exemple, les crimes

commis sur le Web clandestin sont notoirement difficiles à détecter et à contrer. Les opérations de police spécialisées peuvent perturber certaines activités cybercriminelles, mais à long terme, elles n'ont qu'un impact limité sur l'écosystème des cybermenaces dans son ensemble.

Il existe des lacunes importantes dans la législation, la réglementation, les normes et les politiques visant à lutter contre les méfaits en ligne. Par exemple, le contenu intime non consensuel provenant de l'extérieur du Canada complique et prolonge les poursuites au pays. De plus, les outils réglementaires canadiens sont fragmentés ou ambigus. Un exemple notoire est la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui interdit aux organisations privées de recueillir, d'utiliser ou de communiquer des renseignements personnels sans le consentement de la personne; toutefois, elle ne s'applique généralement pas aux activités non commerciales. Les lacunes réglementaires et la confusion entourant la surveillance des sites de sociofinancement hors Canada, ainsi que de certaines formes de plateformes d'échanges de cryptomonnaies, persistent également.

Outre les problèmes de compétence et de réglementation, certains organismes ne disposent pas des pouvoirs d'exécution nécessaires. Par exemple, les commissaires à la protection de la vie privée fédéral et provinciaux ou territoriaux ont pour mandat d'examiner les plaintes pour atteinte à la vie privée, mais leurs pouvoirs d'exécution respectifs varient. La plupart des commissaires ne sont pas en mesure de faire appliquer leurs décisions ou d'accorder une compensation monétaire aux personnes concernées, contrairement aux commissaires d'autres pays. De plus, en vertu de la loi, le Centre d'analyse des opérations et déclarations financières du Canada a pour mandat de lutter contre le blanchiment d'argent et le financement des activités terroristes, mais il ne dispose pas de pouvoirs d'enquête et de collaboration avec les forces de l'ordre équivalents à ceux des organismes similaires au Royaume-Uni et aux États-Unis. Au Canada, la répression des crimes financiers incombe aux services de police, dont la capacité à retracer les transactions dans le cadre d'enquêtes criminelles est limitée, surtout face à l'utilisation croissante des TIC émergentes comme les cryptomonnaies.

Sur le terrain, la pénurie persistante de ressources financières, technologiques et humaines au sein des forces de l'ordre et de l'ensemble du système de justice pénale constitue un obstacle majeur aux enquêtes et aux poursuites contre les crimes cyberfacilités dans les délais impartis. Le Canada ne compte pas suffisamment de ressources et d'expertise spécialisées nécessaires pour traiter le volume croissant de preuves numériques, et le modèle généraliste des corps policiers ne favorise pas le recrutement et la rétention d'agents qui possèdent les compétences requises. Un manque de reconnaissance du rôle des cyberspécialistes travaillant dans l'écosystème policier, associé à leur faible visibilité, peut également accroître les contraintes de capacité. L'une des conséquences de ce

manque d'expertise est que le système de justice pénale est profondément limité dans sa capacité à traiter efficacement la nature de plus en plus numérique de la criminalité et l'augmentation associée des preuves à examiner. Au Canada, les citoyens possèdent le droit constitutionnel d'être jugés dans un délai raisonnable[2], et les retards de traitement des preuves numériques peuvent entraîner la suspension de la procédure, tandis que l'insuffisance des ressources peut conduire à l'abandon pur et simple de certaines affaires. En outre, une mauvaise coordination et une mauvaise compréhension de ce qui peut être partagé au sein des forces de l'ordre et entre elles peuvent provoquer la confusion et une allocation inefficace des ressources.

Les forces de l'ordre canadiennes décrivent souvent les mécanismes actuels d'accès aux preuves et aux données criminelles hébergées à l'étranger comme trop lents, lourds ou exigeants en ressources. De même, le chiffrement a été cité par les forces de l'ordre comme un obstacle aux enquêtes sur les actes criminels, en particulier lorsqu'elles doivent compter sur les fournisseurs de services pour obtenir les preuves pertinentes dans un format accessible. Par contre, l'affaiblissement du chiffrement entraînerait des risques considérables pour la vie privée, car il est essentiel pour protéger les renseignements des utilisateurs.

Parallèlement aux divers acteurs gouvernementaux et de forces de l'ordre, le secteur privé a un rôle important à jouer dans la gouvernance des environnements numériques. Par exemple, les entreprises de médias sociaux s'autorégulent en grande partie lorsqu'il s'agit de modérer le contenu de leurs platesformes et connaissent un succès limité dans la lutte contre le contenu préjudiciable en ligne. Cependant, la mésinformation et le discours haineux sur Internet sont difficiles à contenir parce qu'ils peuvent se propager rapidement à grande échelle; cela est dû, en partie, à la conception actuelle de nombreux algorithmes de médias sociaux, qui amplifient le contenu incendiaire générant plus de réactions. De plus, les politiques de retrait de contenu ne sont pas uniformes entre les platesformes de médias sociaux, et la modération, souvent confiée à l'externe, manque de ressources. Certaines méthodes de modération existantes ou proposées, notamment celles qui font appel à l'automatisation, peuvent mener à une suppression excessive de contenu et sont plus susceptibles de signaler du contenu publié par des membres de groupes marginalisés.

2 Dans une décision rendue en 2016 dans l'affaire R. c. Jordan, la Cour suprême du Canada a statué que le délai entre l'arrestation d'un individu et son procès ne pouvait être supérieur à 18 mois dans les cours provinciales et à 30 mois dans les cours supérieures.

À la lumière de l'impact des avancées en technologies de l'information et des communications à l'échelle mondiale, qu'est-ce que les données probantes et les connaissances actuelles indiquent en ce qui concerne les pratiques prometteuses et exemplaires qui pourraient être appliquées au Canada pour enquêter sur les menaces à la sécurité publique, les prévenir et les contrer, tout en respectant les droits de la personne et la vie privée?

Des réformes des cadres juridiques et politiques s'appliquant au contexte numérique sont en cours dans le monde entier. Bien que le Canada puisse apprendre des approches étrangères, tous les ordres de gouvernement doivent tenir compte de la situation juridique canadienne lorsqu'ils évaluent la mesure dans laquelle ces approches sont adaptées à leur territoire.

L'expérience des pays qui partagent certaines similitudes sociopolitiques avec le Canada peut donner une idée des problèmes et des possibilités découlant de démarches réglementaires différentes. Par exemple, la législation australienne permet au commissaire à la sécurité électronique d'enquêter sur certains méfaits cyberfacilités et de les traiter en dehors du cadre traditionnel des forces de l'ordre, tandis que l'Union européenne a adopté des dispositions concernant un mécanisme de notification et de retrait du contenu illégal qui s'appliquera à certains intermédiaires en ligne dans tous les États membres. Certaines mesures mises en pratique ailleurs ont toutefois conduit à la suppression excessive de contenu légal, voire non préjudiciable, ce qui suscite des inquiétudes pour la liberté d'expression et le respect de la vie privée. Il est nécessaire de prendre en compte ces questions, ainsi que les différences entre les systèmes juridiques et entre les cultures juridiques, pour évaluer dans quelle mesure les approches suivies par d'autres pays conviennent au contexte canadien.

Les réformes législatives seules ne résoudront pas les problèmes posés par les TIC. La structure des forces de l'ordre doit s'adapter à l'évolution du contexte du maintien de l'ordre au Canada, et des changements à petite échelle ne permettront pas de remédier aux importantes pénuries de capacités et de compétences dans la police. Parmi les pratiques prometteuses et émergentes dans ce domaine, citons la professionnalisation du maintien de l'ordre, notamment une plus grande différenciation des rôles au sein des forces de l'ordre — par opposition au recours à des agents de police généralistes —, qui pourrait favoriser le perfectionnement et la rétention d'agents possédant des compétences numériques spécialisées. Une formation abordable et accessible dans les compétences numériques générales, accessible à tous les agents et peu coûteuse, pourrait également améliorer la capacité des forces de l'ordre à enquêter

sur les crimes cyberfacilités. De plus, il existe pour le secteur privé et le milieu universitaire des possibilités de jouer un rôle plus actif dans la formation de la police et, dans le cas du premier, dans le traitement de certains types de preuves numériques. Enfin, des initiatives telles que le Compendium nord-américain sur la classification de la cybercriminalité (NACCC) ont le potentiel de combler les lacunes de données et de faciliter une catégorisation précise et uniforme des crimes et méfaits cyberfacilités entre les différents acteurs et États.

Les TIC ne sont cependant pas seulement utilisées pour perpétrer des méfaits. Les forces de l'ordre utilisent tout un ensemble de technologies numériques pour intervenir face aux actes criminels, les prévenir, les détecter et enquêter à leur sujet. Bien que nombre de ces technologies apportent des avantages considérables, une orientation et une surveillance constantes sont nécessaires, car chaque outil comporte des éléments problématiques sur le plan de l'éthique et du respect de la vie privée. Par exemple, la technologie de reconnaissance faciale est utilisée par les forces de l'ordre au Canada pour identifier des personnes d'intérêt dans le cadre d'enquêtes criminelles, mais elle a également donné lieu à des atteintes à la vie privée et à des problèmes d'équité et de ciblage de groupes marginalisés, lesquels étaient prévisibles. À l'avenir, une réglementation, une surveillance, une transparence et une responsabilisation appropriées en matière d'utilisation des nouvelles technologies peuvent assurer leur intégration et leur déploiement adéquats par les forces de l'ordre canadiennes. En comparaison, des organismes tels que le Comité consultatif néo-zélandais sur les technologies émergentes peuvent constituer un mécanisme d'évaluation critique des conséquences politiques et éthiques des nouvelles technologies avant qu'elles ne soient utilisées par la police.

Bien que de nombreux actes cyberfacilités préjudiciables violent le *Code criminel* du Canada, la criminalisation des activités numériques préjudiciables n'est pas systématiquement appropriée, et elle n'est pas toujours le moyen le plus efficace de lutter contre un méfait en ligne donné ni la méthode d'intervention préférée des victimes et des survivants. Dans certains cas, le droit de la responsabilité délictuelle — une forme de droit privé visant à indemniser les personnes lésées par les actes répréhensibles d'autrui — comporte d'importants recours en cas d'atteinte à la vie privée et peut inciter à adopter un comportement légal en ligne. Bien qu'intenter une poursuite dans ce domaine exige beaucoup de ressources et de temps, l'introduction d'une large cause d'action pour les atteintes à la vie privée sous la forme de délits a été couronnée de succès dans certaines provinces canadiennes. Parmi les autres voies juridiques non criminelles, citons le droit relatif à la diffamation, le droit civil du Québec, la législation sur la protection des renseignements personnels qui régit le recueil des données dans les secteurs public et privé et la législation antipourriel. Toutes ces voies juridiques ont leurs propres difficultés et limites.

Tous les méfaits en ligne n'atteignent pas le seuil du comportement criminel. Si une réforme juridique peut s'avérer nécessaire pour remédier à certains de ces méfaits, dans d'autres cas, des démarches non juridiques seront plus efficaces et répondront mieux aux préférences des victimes et des survivants.

La gouvernance des espaces numériques ne se limite pas aux outils et règles sanctionnés par l'État et, dans certains cas, aucune voie juridique ne convient. Par ailleurs, il existe divers instruments permettant de mettre sur pied un système de gouvernance adaptatif, notamment des politiques d'autogouvernance des entreprises et des codes de conduite volontaires. Certaines grandes entreprises de médias sociaux ont élaboré des politiques qui définissent ce qui est considéré comme du contenu préjudiciable et ont démontré leur capacité à modérer et à supprimer de manière réactive de gros volumes de ce type de contenu sur leurs platesformes dans des cas particuliers. Parmi les autres nouvelles pratiques instaurées par les grandes entreprises de médias sociaux, citons les partenariats avec des entreprises et des institutions tierces de vérification des faits, la constitution de comités d'examen indépendants chargés de prendre des décisions de modération de contenu très médiatisées et l'utilisation d'outils automatisés (bien qu'il ait été démontré que cela conduisait à une suppression excessive de contenu). Malgré ces efforts, le contenu préjudiciable continue de proliférer et d'autres problèmes persistent, comme le manque de transparence, de responsabilité et de cohérence dans les décisions de modération.

Certaines victimes et certains survivants peuvent également préférer des moyens hors du circuit juridique pour remédier aux préjudices cyberfacilités. Par exemple, dans le cas de la diffusion non consensuelle d'images intimes, la priorité immédiate de la victime ou du survivant peut être le retrait de ces images des espaces en ligne, plutôt qu'une enquête criminelle. La prévention, tant du côté de l'auteur que de la cible, peut également avoir un effet. Par exemple, les programmes d'éducation dirigés par les pairs et les initiatives et politiques émanant d'écoles peuvent contribuer à résoudre le problème de harcèlement et d'abus en ligne, en particulier chez les jeunes. De même, il existe des initiatives prometteuses d'éducation à la culture numérique qui peuvent doter les gens des outils nécessaires pour évaluer de manière critique les informations sur Internet, déceler le contenu préjudiciable et réduire les risques pour la vie privée.

Les problèmes de gouvernance sont aggravés par le fait que la protection de la vie privée est très contextuelle et que la conception sociétale de ce qu'est la vie privée évolue constamment. Il est impossible de trouver l'équilibre idéal entre la

Dans les contextes numériques, la protection de la vie privée et les droits de la personne, d'une part, et la sécurité, d'autre part, sont souvent perçus comme étant en contradiction, mais ils peuvent se renforcer mutuellement.

protection de la vie privée et la sécurité, et ce n'est pas non plus un principe approprié aux contextes numériques. Au contraire, il existe souvent une interaction complexe, dynamique et contextuelle entre la vie privée, la sécurité et d'autres droits et libertés, notamment la liberté d'association. Parfois, certaines formes de sécurité supplantent le droit à la vie privée des individus. Il est important de noter que la protection de la vie privée et la sécurité peuvent se renforcer mutuellement, et qu'un certain degré de vie privée est nécessaire pour assurer la sécurité personnelle d'un individu ou la sécurité de la communauté dans laquelle il réside.

Le droit à la vie privée est protégé par le droit canadien, alors que, dans le même temps, la croissance du volume et des genres de renseignements numériques rendent la protection de la vie privée et la sécurité numérique de plus en plus compliquées. Les gouvernements, les forces de l'ordre et les entreprises privées ont considérablement étendu le recueil, l'utilisation et la communication de données, souvent sans consentement, par-delà les frontières et avec une surveillance limitée. Les outils réglementaires actuels destinés à protéger et à régir la gestion des renseignements personnels doivent être réformés et renforcés de manière coordonnée et transparente. Dans ce contexte, il est également essentiel que les individus et les communautés aient la possibilité de prendre des décisions éclairées au sujet de leur vie privée. Certaines provinces ont élaboré leurs propres méthodes en matière de protection de la vie privée. Par exemple, la *Charte des droits et libertés de la personne* du Québec reconnaît la vie privée comme un droit de la personne, qu'elle garantit en offrant un droit de poursuite direct aux personnes concernées. De même, la loi québécoise sur la protection de la vie privée dans le secteur privé a une portée plus large et des mesures d'application plus strictes que la législation fédérale similaire.

Quelles sont les possibilités d'améliorer la santé globale de l'écosystème en ligne (par exemple, soutenir la résilience des platesformes et des services face à l'exploitation)?

Il n'existe pas de panacée lorsqu'il s'agit d'améliorer la santé globale des écosystèmes numériques, ni d'acteur unique capable de protéger la sécurité publique en ligne. Il existe divers mécanismes juridiques et non juridiques dans lesquels les différents ordres de gouvernement, les forces de l'ordre, les entreprises privées, la société civile, les établissements d'enseignement et les

individus jouent tous un rôle important pour renforcer la résilience aux préjudices en ligne. Bien que les entreprises de médias sociaux aient pris certaines mesures pour modérer le contenu répréhensible et haineux, un volume considérable de contenu préjudiciable subsiste; il est toutefois possible de continuer à innover, à s'adapter et à collaborer préventivement. Il est essentiel à tout effort visant à améliorer la santé de l'écosystème numérique de réellement associer les victimes et les survivants et adopter des approches centrées sur les victimes et qui tiennent compte de leurs traumatismes.

Des investissements et des interventions précoces prenant en considération les droits de la personne ont permis au Canada d'enquêter et d'intenter des poursuites plus efficacement pour certains crimes cyberfacilités.

Dans le cadre de la gouvernance publique des espaces numériques, certaines politiques émergentes cherchent à établir des mécanismes suffisants pour dissuader les individus d'agir illégalement, sans pour autant empiéter indûment sur la liberté d'expression et la vie privée des utilisateurs. Toutefois, comme le démontrent les approches réglementaires existantes et proposées au Canada et à l'étranger, il est difficile de concilier entièrement ces principes, en partie parce que les technologies numériques évoluent rapidement.

Nombre des obstacles qui empêchent de répondre adéquatement aux méfaits cyberfacilités sont systémiques et nécessitent des réformes substantielles. Les démarches nouvelles et prometteuses entreprises par différents pays, provinces et secteurs offrent de précieuses leçons au Canada. Si ce rapport regorge d'exemples de la manière dont les outils technologiques peuvent être utilisés par divers acteurs pour commettre des actes préjudiciables, la technologie peut également faire partie de la solution, en combinaison avec une méthode de gouvernance collective et transnationale qui comprend une transparence et une surveillance appropriées. Dans l'ensemble, le maintien d'un écosystème numériques plus sûr ne se fera pas uniquement à l'aide de mesures graduelles ou par l'action d'une seule entité. L'amélioration de la sécurité publique numérique des individus au Canada exige une approche collective qui réunit la société civile, les décideurs, les forces de l'ordre et le secteur privé, et comprend des mécanismes juridiques et non juridiques.

Abréviations

IA	intelligence artificielle
RBA	renseignements de base sur les abonnés
CCPE	Centre canadien de protection de l'enfance
LCAP	Loi canadienne antipourriel
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
MAP	matériel d'abus pédosexuels
SCRS	Service canadien du renseignement de sécurité
ACEUM	Accord Canada-États-Unis-Mexique
DEX	des plateformes d'échange décentralisées
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
TRF	technologie de reconnaissance faciale
RGPD	Règlement général sur la protection des données
TIC	technologies de l'information et des communications
EVCI	extrémisme violent à caractère idéologique
AEJ	accord d'entraide juridique
TAJ	traité d'entraide juridique
ESM	entreprise de services monétaires
NACCC	Compendium nord-américain sur la classification de la cybercriminalité
FSCL	fournisseur de services de communication en ligne
ODIT	outil d'enquête intégré
CPVP	Commissariat à la protection de la vie privée du Canada
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
EVCP	extrémisme violent à caractère politique
EVCR	extrémisme violent à caractère religieux
CTEV	contenu terroriste et extrémiste violent
RPV	réseau privé virtuel

Table des matières

1

Introduction

Le développement et la prolifération des systèmes en ligne ont permis de réaliser des progrès immenses, grâce notamment à des méthodes de communication, de recueil de données et d'analyse plus accessibles et plus puissantes. Internet et les technologies de l'information et des communications (TIC) qui y sont associées (y compris les médias sociaux et d'autres applications Web) sont essentiels au quotidien des personnes vivant au Canada — et leur omniprésence fait que tout le monde au pays est *numérique par défaut*, qu'il soit en ligne ou non. Mais les systèmes en ligne permettent également aux acteurs malveillants d'infliger de graves préjudices aux personnes et aux communautés. Ce rapport examine la nature de ces menaces en ce qui concerne la sécurité, la vie privée et les droits de la personne de la population canadienne.

À mesure que les activités et les informations se déplacent vers Internet, les gens sont de plus en plus sensibles et vulnérables aux cybermenaces et à la cybercriminalité. Cette situation n'est pas seulement coûteuse pour les organisations et les particuliers; la criminalité facilitée par la technologie et les activités en ligne nuisibles constituent également une menace pour la sécurité et le bien-être des individus au Canada et à l'étranger. Ce rapport étudie la nature constamment évolutive des TIC et les problèmes et possibilités qu'elles représentent pour tous les ordres de gouvernement, pour les forces de l'ordre et pour les autres acteurs qui s'efforcent de prévenir et de combattre les comportements illégaux et préjudiciables.

1.1 Mandat

Admettant l'importance de connaître et de résoudre les difficultés posées par les TIC, Sécurité publique Canada (ci-après « le commanditaire ») a demandé au Conseil des académies canadiennes (CAC) de constituer un comité d'experts chargé d'examiner les pratiques exemplaires qui pourraient contribuer à réduire les risques pour la sécurité publique tout en respectant les droits de la personne et la vie privée. Le CAC avait plus précisément pour mandat de répondre à la question et aux sous-questions suivantes :

À la lumière de l'impact des avancées en technologies de l'information et des communications à l'échelle mondiale, qu'est-ce que les données probantes et les connaissances actuelles indiquent en ce qui concerne les pratiques prometteuses et exemplaires qui pourraient être appliquées au Canada pour enquêter sur les menaces à la sécurité publique, les prévenir et les contrer, tout en respectant les droits de la personne et la vie privée?

- Comment les activités criminelles graves (notamment le crime organisé et l'exploitation sexuelle des enfants) et causant des préjudices en ligne (notamment la désinformation, l'utilisation d'Internet à des fins extrémistes violentes et terroristes) au Canada ont-elles évolué pour exploiter le paysage changeant des technologies de l'information et des communications (TIC)?
- Quels défis les progrès des TIC (notamment le chiffrement et la 5G) posent-ils pour la prévention, la lutte, les enquêtes et les poursuites relatives aux crimes et pour l'atténuation des préjudices en ligne?
- Quelles sont les possibilités d'améliorer la santé globale de l'écosystème en ligne (par exemple, soutenir la résilience des platesformes et des services face à l'exploitation)?

1.2 Approche du comité d'experts

Pour répondre aux questions qui précèdent, le CAC a formé un comité multidisciplinaire de 13 experts (le comité d'experts sur la sécurité publique à l'ère du numérique) possédant de l'expérience et une expertise en cybersécurité, en sciences sociales, en criminologie, en forces de l'ordre et en droit et gouvernance. Chacun d'eux a agi à titre de personne informée plutôt que comme représentant d'une discipline, d'un organisme, d'une région ou d'un ensemble de valeurs en particulier. Le comité d'experts s'est réuni plusieurs fois virtuellement et une fois en personne en 12 mois afin d'examiner et de recueillir les données probantes et de délibérer sur son mandat.

Au début du processus, le comité a rencontré le commanditaire afin de bien comprendre son mandat et de confirmer les éléments inclus et non inclus dans la portée de l'évaluation. Le commanditaire a mentionné qu'il souhaitait que le comité d'experts se penche sur les activités cyberfacilitées (*cyber-enabled*) et préjudiciables graves qui influent directement sur la vie des gens dans les espaces non numériques au Canada. Il a également précisé que les cybercrimes purs, dans lesquels la technologie elle-même est ciblée (p. ex. la divulgation de données) n'entraient pas dans le champ de l'évaluation. Par conséquent, le rapport se focalise sur les activités cyberfacilitées les plus dommageables pour les individus plutôt qu'uniquement sur le sous-ensemble d'activités considérées comme criminelles (figure 1.1). En d'autres

termes, le comité d'experts a axé son travail sur les activités et les pratiques — facilitées par les TIC — qui causent, ou qui ont le potentiel de causer, le plus de tort aux gens au Canada, qu'elles soient signalées ou considérées juridiquement comme des crimes. Il est à noter qu'un grand nombre de ces menaces (mais pas toutes) sont posées par le biais de services qui dépendent du contenu généré par les utilisateurs.

Ce raisonnement s'explique en partie par le fait que la frontière entre ce qui est criminel et ce qui est préjudiciable est souvent floue, particulièrement dans le cas des activités menées au moyen des TIC. De plus, ce qui est considéré comme un crime varie selon l'époque et le pays. Par exemple, bien que les répercussions négatives de la cyberintimidation soient bien documentées, seuls certains actes de cyberintimidation (p. ex. le harcèlement criminel, les menaces) sont contraires à la loi au Canada (SP, 2021a). Il en va de même pour le discours haineux; bien que la propagande haineuse figure dans le *Code criminel*, il peut être difficile de déterminer le point où le discours haineux franchit le seuil de ce qui constitue une infraction criminelle, ce qui peut rendre les poursuites difficiles.

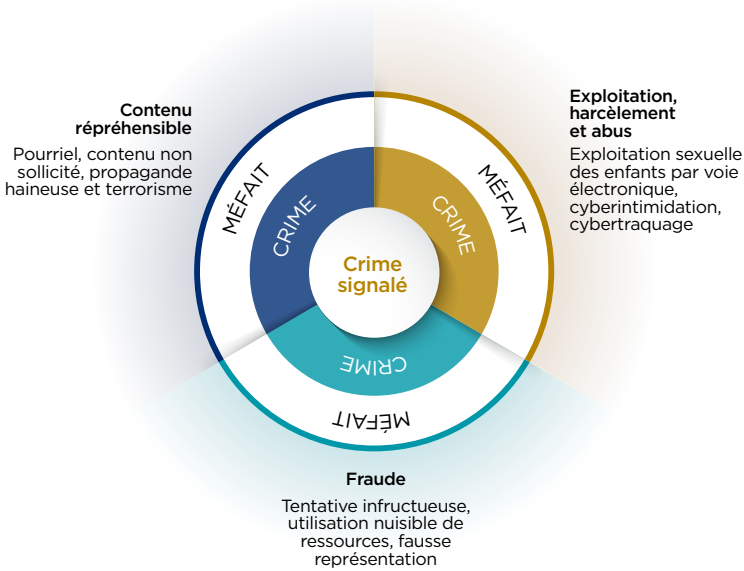


Figure 1.1 Conceptualisation de l'univers des préjudices

Ce qui est légalement considéré comme un acte criminel varie selon l'époque et le pays et ne rend pas compte de tous les préjudices subis en ligne. Dans le même temps, on sait que les crimes signalés ne représentent qu'un sous-ensemble de tous les actes criminels cyberfacilités. La portée de ce rapport est limitée aux types de méfaits qui seraient considérés comme des crimes et méfaits cyberfacilités (technologie en tant qu'instrument), selon la définition de la division sur la cybercriminalité du Compendium nord-américain sur la classification de la cybercriminalité (NACCC) — c'est-à-dire les méfaits dans lesquels la technologie numérique est utilisée afin de cibler des personnes.

En outre, à la demande du commanditaire, des sujets tels que la mésinformation, les croyances complotistes et la diffusion de contenus extrémistes ou haineux sont traités dans ce rapport en raison des effets perturbateurs et nuisibles qu'ils peuvent avoir sur le discours public, et parce qu'ils peuvent faciliter les mouvements et les actes susceptibles de menacer le public ou de lui nuire.

1.3 Contextualisation du mandat

Ce rapport porte sur les crimes et méfaits cyberfacilités qui menacent la sécurité des individus

Dès le départ, le comité d'experts a souligné l'importance de contextualiser les activités criminelles et nuisibles d'origine cybernétique, tant sur le plan historique que social. Tout au long de l'histoire, les progrès technologiques ont modifié les cibles des crimes, les types de crimes commis, les méthodes pour les commettre et les méthodes et outils de forces de l'ordre employés pour prévenir et combattre la criminalité (Brey, 2017). Les TIC (et la technologie dans son ensemble) ont historiquement bénéficié à la fois aux acteurs malveillants et aux forces de l'ordre (Brey, 2017). De même, il existe un historique bien documenté d'inquiétudes relatives aux diverses technologies susceptibles de permettre le crime, ainsi que de craintes que la technologie puisse être utilisée pour le contrôle sociétal (McGuire, 2017).

Sur le plan sociologique, Brey (2017) affirme que les TIC reproduisent (sous forme numérique) nombre d'actions, d'objets, de valeurs, de pratiques et d'institutions sociaux qui existent déjà. Par conséquent, les comportements en ligne (y compris les comportements criminels) sont souvent un prolongement de ce qui se produit hors ligne, quand ce ne sont pas exactement les mêmes comportements transposés au Web (Lukings et Lashkari, 2022b). De ce point de vue, il n'est pas surprenant que de nombreux crimes et méfaits autrefois commis hors ligne (p. ex. la fraude ou l'exploitation des enfants) aient migré vers les platesformes numériques (Brey, 2017). De même, l'émergence de la cybercriminalité et des méfaits cyberfacilités peut être le résultat de nombreux facteurs, dont certains ne sont pas liés à la prolifération des TIC, notamment l'accroissement de la polarisation sociétale et de l'isolement (Centre canadien d'engagement communautaire et de prévention de la violence, 2018; Waller et Anderson, 2021).

Si les TIC ont entraîné une évolution de la criminalité et des comportements préjudiciables, elles offrent également de nombreux avantages pour la société. Elles sont cruciales pour l'accès aux services essentiels (p. ex. l'éducation, les soins de santé), le fonctionnement de l'économie (p. ex. la participation au marché du travail, le magasinage, l'innovation, les activités commerciales), le maintien des liens sociaux et l'accès à l'information (CAC, 2021; StatCan, 2021a). Les forces de

l'ordre utilisent également les TIC et en dépendent pour intervenir face aux crimes, enquêter dessus, les prévenir et communiquer à leur sujet (GRC, 2020a; FBI, 2022). En outre, les technologies numériques sont importantes pour le respect des droits de la personne et la réalisation des objectifs démocratiques. Par exemple, un rapport du rapporteur spécial du Conseil des droits de l'homme des Nations Unies a constaté que les TIC sont des outils clés qui aident les gens à exercer des droits fondamentaux, tels que la liberté d'opinion et d'expression (CDH, 2011a). Des outils comme le chiffrement permettent aux défenseurs des droits de la personne, aux journalistes et autres d'échanger et de stocker des renseignements et des données en toute sécurité (Parsons, 2019). Ces questions sont étudiées au chapitre 2.

Les crimes cyberfacilités sont en hausse, mais sont aussi sous-déclarés au Canada

Si les technologies numériques procurent des avantages considérables, elles peuvent également entraîner des préjudices importants, notamment une augmentation des actes qualifiés de crimes cyberfacilités. Bien que de nombreux cas de cybercrimes ne soient pas signalés, il est prouvé que la fréquence des cybercrimes et le nombre d'auteurs de cybermenaces au Canada augmentent (GRC, 2014; Centre canadien pour la cybersécurité, 2020a; Lukings et Lashkari, 2022b). Dans le même temps, le Centre canadien pour la cybersécurité (2022a) relève que « la cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher les Canadiens et les organisations canadiennes ».

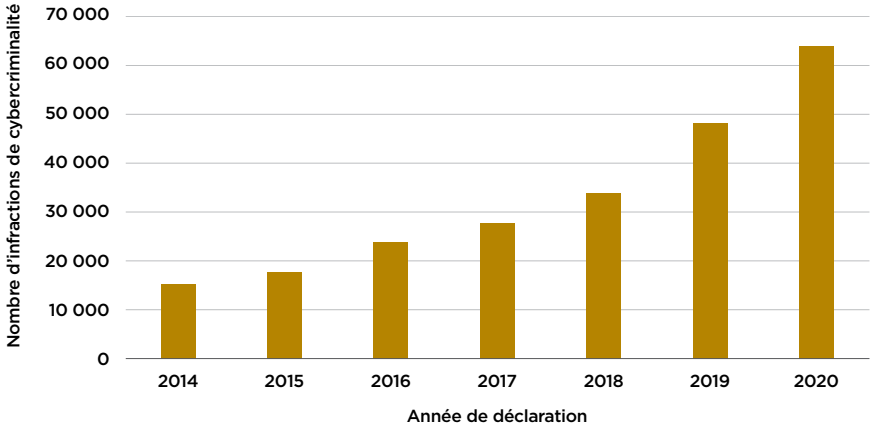
Le nombre de cybercrimes déclarés a augmenté chaque année depuis 2014, année à laquelle Statistique Canada a commencé à communiquer ces chiffres selon une méthodologie établie[1] (StatCan, 2021b). En 2020, 63 523 infractions cybercriminelles ont été déclarées à la police au Canada, ce qui constitue une augmentation de plus de 400 % par rapport à 2014 (StatCan, 2021b) (figure 1.2). Cela dit, les cybercrimes signalés à la police ne représentent qu'une petite partie des crimes déclarés au Canada. Par exemple, une étude a constaté une moyenne de 44 occurrences de cybercriminalité pour 100 000 personnes, contre près de 5 000 pour 100 000 personnes pour l'ensemble des crimes — infractions au code de sécurité routière exclues — dans les huit plus grosses municipalités du Canada entre 2014 et 2017 (Popham *et al.*, 2020).

L'augmentation de la cybercriminalité entre 2020 et 2022 peut être attribuée à plusieurs facteurs (liés ou non à la pandémie de COVID-19), notamment un accès plus facile et moins coûteux aux TIC et à la connectivité Internet dans la plupart

1 Statistique Canada définit la *cybercriminalité* comme « toute infraction relevant du *Code criminel* du Canada dans laquelle la technologie de l'information et des communications (TIC) est l'objet du crime, ou dans laquelle la TIC est nécessaire à la perpétration de l'infraction et en fait partie intégrante » (CCSJSC, 2021). Cette définition inclut les crimes cyberfacilités qui sont au cœur du présent rapport.

des pays (Lukings et Lashkari, 2022b) et un isolement social et une polarisation sociétale croissants (Waller et Anderson, 2021). On sait que les Canadiens ont passé plus de temps en ligne pendant la pandémie, car de nombreux aspects de la vie quotidienne se sont déplacés dans cette sphère (StatCan, 2020a), créant ainsi plus de possibilités pour les auteurs de cybermenaces (Moreau, 2021a).

Au Canada, près de la moitié des cybercrimes signalés à la police en 2020 concernaient la fraude (StatCan, 2021b) (section 3.3). Après la fraude, les cybercrimes correspondant au mandat du comité d'experts les plus souvent signalés par la police sont les communications indécentes ou harcelantes, la production ou la distribution en ligne de matériel d'abus pédosexuel (MAP) et les menaces (StatCan, 2021b). L'incidence du signalement de toutes les catégories de cybercriminalité augmente toutefois (Centre antifraude du Canada, 2021a; Dupont, 2021). Par exemple, les menaces proférées en ligne (signalées à la police) ont augmenté de près de 500 % entre 2014 et 2020 (StatCan, 2021b).



Source des données : StatCan (2021b)

Figure 1.2 Nombre d'infractions de cybercriminalité déclarées à la police au Canada

Le nombre d'infractions de cybercriminalité déclarées à la police chaque année au Canada a augmenté depuis que Statistique Canada a commencé à communiquer ce chiffre. Une infraction de cybercriminalité est une infraction dans laquelle un ordinateur ou Internet était la cible du crime ou l'instrument utilisé pour commettre le crime.

Les données portent à croire que la plupart des victimes de cybercrimes ou des survivants sont des femmes et des mineurs, tandis que la plupart des auteurs sont des hommes

Si tout le monde peut être la cible d'un préjudice cyberfacilité, la fréquence et l'impact de ce type d'acte ne sont pas les mêmes pour tous les groupes sociodémographiques. Les informations publiques les plus récentes et les plus complètes sur les caractéristiques des victimes ou des survivants de cybercrimes au Canada ont été recueillies en 2012, et ne portent que sur les crimes déclarés à la police (Mazowita et Vézina, 2014). Cette année-là, 69 % des victimes ou survivants d'incidents violents de cybercriminalité signalés par la police étaient des femmes; de même, 84 % des victimes ou survivants de cybercriminalité sexuelle étaient des femmes. Dans l'ensemble, en 2012, 42 % des victimes ou des survivants de la cybercriminalité signalés par la police au Canada avaient moins de 18 ans. La plupart (96 %) des victimes ou survivants d'infractions sexuelles associées à la cybercriminalité avaient moins de 18 ans, et 10 % avaient 12 ans ou moins (Mazowita et Vézina, 2014). D'autres statistiques concernant des types particuliers de cybercrimes et de méfaits se trouvent dans les chapitres suivants.

Les entreprises et les organismes font également partie des cibles de la cybercriminalité, bien qu'une grande partie des actes les visant ne soient pas déclarés (Wanamaker, 2019). Une enquête menée auprès d'entreprises canadiennes a montré que, parmi les attaques déclarées de cybercriminalité contre les entreprises, la plupart avaient pour but le vol d'argent ou une demande de rançon. Cependant, de nombreux autres cybercrimes ciblant les entreprises ont impliqué le vol de données personnelles et financières de clients (Wanamaker, 2019).

Au Canada, les hommes représentent la majorité (76 %) des personnes accusées de cybercrimes (Mazowita et Vézina, 2014). La proportion grimpe à 94 % lorsque les cybercrimes sont de nature sexuelle. Souvent, cependant, aucun suspect n'est identifié dans les affaires de cybercriminalité, et nombre d'entre elles ne sont jamais résolues. En 2012, par exemple, aucun suspect n'a été identifié dans 69 % des infractions de cybercriminalité sexuelle et 45 % des infractions de cyberintimidation signalées (Mazowita et Vézina, 2014).

L'écosystème de la cybermenace et les motivations des auteurs de cybermenaces sont complexes

Les auteurs de cybermenaces peuvent être des individus, des groupes, des organisations ou des États ayant l'intention malveillante de nuire au bien-être ou à la sécurité des personnes (Centre canadien pour la cybersécurité, 2021a). Ils peuvent également avoir des motivations politiques ou idéologiques. Leur emplacement, le degré de perfectionnement de leurs techniques et de leur logistique, les ressources dont ils disposent, leur formation et le soutien dont bénéficient leurs activités varient. Les motivations des auteurs de cybermenaces

diffèrent également (Centre canadien pour la cybersécurité, 2021a), même si le comité d'experts note qu'un acteur donné peut être animé par plusieurs motivations, notamment la satisfaction personnelle, des facteurs géopolitiques, le mécontentement, le divertissement, le profit, la violence idéologique et autres éléments idéologiques (figure 1.3). En outre, comme pour les espaces numériques dans leur ensemble, l'écosystème de la cybermenace est lui-même en constante évolution (Centre canadien pour la cybersécurité, 2022a).

Selon Dupont (2019), l'espace de cybersécurité est le lieu d'interactions entre trois communautés interdépendantes :

- Une communauté industrielle (qui introduit souvent des progrès et des risques numériques);
- Une communauté criminelle (qui exploite les progrès numériques à des fins criminelles);
- Une communauté de la sécurité (p. ex. forces de l'ordre, organisations internationales).

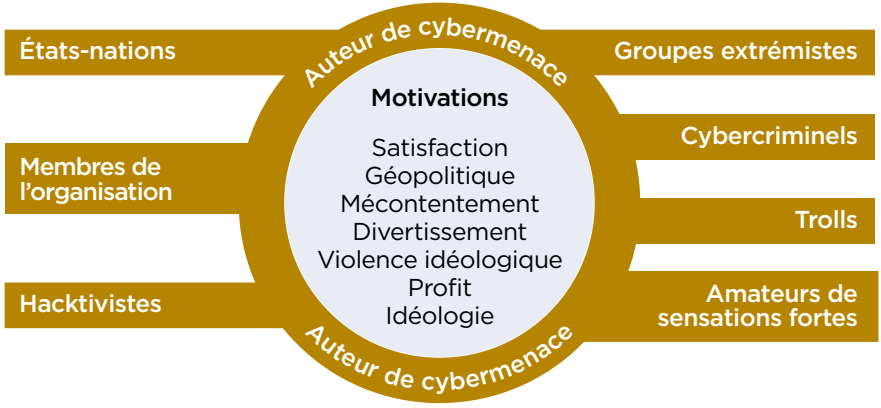


Figure 1.3 Les différents types d'auteurs de cybermenaces et leurs motivations

Les auteurs de cybermenaces peuvent être des États, des groupes, des organisations ou des individus qui commettent malicieusement des activités illégales ou autrement préjudiciables en ligne. Ils peuvent être situés physiquement n'importe où dans le monde et peuvent être animés par une ou plusieurs des motivations répertoriées.

À cet égard, une analyse des réseaux sociaux mondiaux a montré que, sur les 657 acteurs organisationnels de la cybersécurité étudiés, près de la moitié appartenaient au secteur privé, suivis des acteurs nationaux des forces de l'ordre et de la justice (31 %) et des organismes non gouvernementaux et professionnels (16 %) (Dupont, 2016). Cette répartition porte à croire qu'il existe des modèles de gouvernance polycentriques de la cybercriminalité, dans lesquels plusieurs centres prennent des décisions de manière semi-autonome. Cependant, cette analyse omet les efforts de la société civile, qui contribue de différentes manières (p. ex. en créant des organisations dirigées par la communauté, en produisant des études et des rapports, en plaidant pour sa protection). Maschmeyer *et al.* (2021) avancent que le peu d'importance accordée aux préjudices causés à la société civile est le résultat de multiples facteurs qui incitent le secteur de la cybersécurité à protéger les entités très en vue qui possèdent les ressources nécessaires pour payer des dispositifs de cyberdéfense haut de gamme.

1.3.1 Domaines d'intérêt et terminologie

Les auteurs de menaces *cyberfacilitées* utilisent la technologie numérique pour nuire aux personnes

L'étendue des menaces et des méfaits que l'on peut considérer comme *cyberfacilités* est vaste et inclut des activités qui entrent ou non dans le cadre des travaux du comité d'experts. Du point de vue du maintien de l'ordre au Canada, le *cybercrime* est généralement défini comme « n'importe quel type de crime commis en grande partie à l'aide d'Internet et des technologies de l'information, comme des ordinateurs, des assistants numériques personnels ou des appareils mobiles » (GRC, 2014). En ce qui concerne les cybercrimes, on différencie généralement les crimes cyberfacilités des crimes cyberdépendants (*cyber-dependant*). Les crimes cyberdépendants ciblent la technologie. Ils sont également connus comme des infractions où la *technologie est la cible* et « ne peu[ven]t être commis qu'au moyen d'ordinateurs, de réseaux ou d'appareils numériques »; citons par exemple le piratage et la propagation de logiciels malveillants (GRC, 2021a). En revanche, les crimes cyberfacilités — également connu sous l'appellation *d'infractions où la technologie est l'instrument* ou de *crimes cyberassistés* — ciblent principalement les gens. Si ces crimes entrent généralement dans la catégorie des crimes pouvant être commis sans les TIC, ils peuvent prendre de l'ampleur quand ils sont commis au moyen de la technologie (INTERPOL, 2021; GRC, 2021a). Toutefois, les activités illégales ne sont pas toutes criminelles, et les activités préjudiciables ne sont pas toutes illégales. Pourtant, des activités préjudiciables, mais légales peuvent tout de même constituer des menaces à la sécurité publique. Pour cette raison, ce rapport porte aussi sur les activités qui n'atteignent pas nécessairement le seuil de l'illégalité. En outre, le comité d'experts relève que l'État où ces activités se déroulent influence le droit applicable et les mécanismes d'application (p. ex. droit criminel, droit de la responsabilité délictuelle, common law) (encadré 1.1).

De nombreuses menaces traditionnellement hors ligne ont été adaptées à l'écosystème en ligne

Conformément aux intérêts du commanditaire, les recherches et l'analyse du comité d'experts ont porté sur les activités préjudiciables qui sont généralement considérées comme cyberfacilitées[2]. De nombreuses activités relevant de la portée de ce rapport brouillent la ligne de démarcation entre les méfaits en ligne et les méfaits analogues *traditionnellement* hors ligne qui ont été adaptés ou améliorés au moyen de la technologie. Par exemple, la police rapporte que certains voleurs de voiture placent de petits dispositifs de suivi sur des véhicules haut de gamme stationnés dans des lieux publics afin de pouvoir les repérer plus tard pour les voler (YRP, 2021). Un autre exemple est la fraude commise après le piratage du téléphone, de l'ordinateur ou du réseau d'une personne afin de recueillir des données personnelles (INTERPOL, 2021). À cause de l'utilisation répandue des TIC, on peut s'attendre à ce que la plupart des crimes aient une certaine composante numérique (Beesley, 2021).

Les choix terminologiques effectués par le comité d'experts, y compris ceux concernant les gens qui souffrent des effets des activités décrites dans ce rapport, sont expliqués dans l'encadré 1.1.

Encadré 1.1 Terminologie employée par le comité d'experts

- **infraction criminelle** — Acte ou omission perpétré contre l'État ou contre l'ordre public et punissable en vertu du droit criminel.
- **crime cyberfacilité** — Infraction criminelle commise au moyen de la technologie.
- **méfait cyberfacilité** — Infraction criminelle ou autre acte préjudiciable illégal ou légal commis au moyen de la technologie.
- **forces de l'ordre** — Organismes chargés de mettre en application les lois canadiennes au pays. Cela inclut les quatre échelons de services policiers canadiens : national, provincial, municipal et autochtone. Les forces de l'ordre ne sont qu'une catégorie d'*organismes de sécurité publique*, qui incluent également les services de renseignement, les services frontaliers, le service correctionnel et les services de libération conditionnelle.

(Continue)

2 Si le comité d'experts note que les menaces considérées comme *cyberdépendantes* peuvent aussi causer d'importants préjudices aux individus, elles ne font pas l'objet du présent rapport.

(a continué)

- **platesformes en ligne —** Ensemble de services Internet, dont les médias sociaux, les places de marché en ligne, les services de partage de contenu et les moteurs de recherche. Ces services utilisent généralement les TIC pour connecter les utilisateurs les uns aux autres, tout en recueillant souvent des données sur ces derniers et sur leur activité en ligne. Les platesformes en ligne ne sont généralement pas conçues pour faciliter l'*interopérabilité entre les platesformes* (p. ex. les utilisateurs de Facebook ne peuvent pas envoyer des messages aux utilisateurs de Twitter) ni pour offrir des options de *portabilité des données*, qui permettraient aux utilisateurs de déplacer des données d'une plateforme à une autre.
- **réglementation —** Selon le contexte, terme utilisé pour faire référence aux règles promulguées par des organismes administratifs en vertu de lois d'habilitation (p. ex. réglementation sur les produits de la criminalité (blanchiment d'argent) et sur le financement du terrorisme) ou à un système de règles applicable à un certain domaine d'activité (p. ex. réglementation des médias sociaux). Dans l'Union européenne, les règlements sont des actes législatifs contraignants qui doivent être appliqués dans leur intégralité par tous les États membres (p. ex. *Règlement général sur la protection des données*).
- **délit —** Acte ou omission qui cause un préjudice ou une blessure à une personne et entraîne un tort pour lequel les tribunaux imposent une responsabilité civile.
- **victime, cible, survivant —** Les crimes et préjudices cyberfacilités traités dans ce rapport ciblent les personnes de toutes les catégories démographiques d'une façon qui peut être émotionnellement douloureuse et difficile à examiner. Les personnes ainsi ciblées peuvent se sentir vulnérables, exploitées et victimes, mais chaque expérience est unique. Il n'existe pas de façon unique de surmonter ces sentiments, car être qualifié de *victime* ou de *survivant* n'est pas représentatif de l'expérience vécue; pour certains, le fait de passer du statut de victime à celui de survivant peut être encourageant (Pollino, 2021). Si le comité d'experts a adopté certains termes pour ce rapport dans un souci de cohérence, il a cherché à être sensible aux expériences uniques de celles et ceux qui ont été la cible des attaques. Pour cette raison, le lecteur constatera que le rapport utilise des termes tels que *cible*, *victime* ou *survivant* dans diverses sections.

Outre les termes décrits dans l'encadré 1.1, le comité d'experts utilise tout au long du rapport les termes *méfait* ou *préjudice* et *cyberméfait* ou *cyberpréjudice*[3], lesquels englobent un éventail d'atteintes au bien-être et aux intérêts d'une personne ou d'une entité (Agrafiotis *et al.*, 2018). À partir d'un examen systématique, Agrafiotis *et al.* (2018) proposent une taxonomie complète des cyberpréjudices qui comprend les préjudices physiques (p. ex. blessure, douleur, décès), les préjudices économiques (p. ex. perte financière, perte d'emploi), les préjudices psychologiques (p. ex. l'anxiété, la dépression), les préjudices pour la réputation (p. ex. relations endommagées, occasions réduites) et les préjudices sociétaux (p. ex. perturbation de la vie quotidienne, répercussions négatives sur une nation). Bien que cet éventail de préjudices corresponde à des impacts négatifs substantiels, en raison des priorités du commanditaire, ce rapport se concentre sur les préjudices physiques, psychologiques, sociétaux et, dans une moindre mesure, économiques à l'échelle individuelle. De plus, alors que le mandat laisse entendre qu'il existe une démarcation entre le monde numérique et le monde non numérique, le comité d'experts ne fait pas cette distinction pour ce qui est des préjudices et des conséquences potentielles.

Dans la mesure du possible, le rapport utilise la terminologie du Compendium nord-américain sur la classification de la cybercriminalité (NACCC)

En raison de la complexité et de l'évolution des cyberméfaits, il n'est pas surprenant que la terminologie utilisée par les différentes forces de l'ordre, les victimes et survivants, la société civile et le système de justice pénale varie (INTERPOL, 2021; NACCC, 2021a). Les problèmes créés par ces variations de définition sont reconnus depuis longtemps au Canada (Kowalski, 2002). Afin de tenter de relever ce défi en ce qui concerne les activités considérées comme criminelles, le Cybercrime Support Network (un organisme américain à but non lucratif), l'Association canadienne des chefs de police et le l'E-Crime Cyber Council, avec l'aide d'un groupe d'experts internationaux en cybercriminalité, ont créé le Compendium nord-américain sur la classification de la cybercriminalité (NACCC) (CNACC, 2021a). Le NACCC cherche à faciliter la catégorisation précise et cohérente des cyberincidents entre plusieurs acteurs et États et peut également servir à catégoriser de manière générale les types de méfaits (NACCC, 2021a). Son système de classification et de terminologie divise les incidents préjudiciables d'origine cybernétique (ceux qui causent des préjudices ou qui comportent des activités illégales) en neuf catégories, elles-mêmes divisées en sous-catégories correspondant à la gouvernance canadienne, américaine et européenne des cybercrimes et autres activités préjudiciables (NACCC, 2021b; Parker, 2021).

3 Le *méfait* est l'acte, tandis que le *préjudice* en est la conséquence [NdT].

Tout au long du présent rapport, le comité d'experts utilise la terminologie du NACCC pour décrire les méfaits qui relèvent des crimes *cyberfacilités*, notamment la publication de contenu répréhensible, l'exploitation, le harcèlement et les abus, ainsi que la fraude (figure 1.1). Le rapport ne couvre toutefois pas les préjudices cyberdépendants (p. ex. utilisation de logiciels malveillants, intrusion, recueil de renseignements, divulgation de données et attaques contre la disponibilité des systèmes et des services). Le comité d'experts fait remarquer que d'autres systèmes de classification et d'autres terminologies sont employés dans les publications; s'il ne cautionne pas un système de classification particulier, il a choisi le NACCC pour assurer une cohérence à l'intérieur du rapport[4].

1.3.2 Sources des données probantes

Les données probantes utilisées pour élaborer ce rapport proviennent de diverses sources et ne se limitent pas aux publications examinées par les pairs

L'évaluation du comité d'experts est fondée sur un examen de diverses sources de données probantes tirées de publications examinées par les pairs, de renseignements et de données gouvernementales accessibles au public, du journalisme d'enquête, de commentaires formulés au sujet de projets de loi, d'entretiens informationnels avec des experts et autres éléments de documentation parallèle[5] touchant la sécurité publique numérique au Canada. Afin d'éclairer son étude des pratiques prometteuses et exemplaires, le comité d'experts a examiné les données probantes provenant d'autres pays (chapitre 5). Ce rapport a également fait l'objet d'un examen approfondi par des pairs, au cours duquel d'autres experts canadiens et internationaux ont produit des données probantes et des conseils supplémentaires.

Le comité d'experts s'est heurté aux limites des données relatives aux cyberméfaits

S'il existe des données claires démontrant la hausse de la cybercriminalité, il est difficile de dresser un tableau précis de sa fréquence et de ses effets, même pour les crimes déclarés, sans parler des méfaits qui n'atteignent pas le seuil de l'illégalité. Comme indiqué précédemment, les cybercrimes ne sont pas définis de manière uniforme, et leurs impacts sont difficiles à quantifier (Furnell *et al.*, 2015).

4 À noter que le NACCC n'existe qu'en anglais. La terminologie utilisée dans la version française du rapport est tirée des principales publications en français sur le sujet [NdT].

5 « Le terme documentation parallèle désigne de nombreux types de documents produits par tous les ordres de gouvernement, par les universitaires, les entreprises et l'industrie, en format imprimé et électronique, qui sont protégés par des droits de propriété intellectuelle, et qui sont d'une qualité suffisante pour être colligés et conservés par les fonds des bibliothèques ou les dépôts institutionnels, mais qui ne sont pas contrôlés par des éditeurs commerciaux, c'est-à-dire pour lesquels l'édition n'est pas l'activité principale de l'organisme qui les a produits [traduction libre] (Schöpfel, 2019).

Par exemple, la cybercriminalité, y compris le crime cyberfacilité, ne figure pas parmi les options proposées dans certains outils canadiens de signalement des crimes (Malone, 2021), et le signalement varie considérablement d'une municipalité à l'autre (Popham *et al.*, 2020). Le comité d'experts constate qu'il incombe généralement aux municipalités d'effectuer le suivi des données sur la criminalité les concernant, au moyen d'un des nombreux systèmes de gestion de rapports; toutefois, ces systèmes ne comportent généralement qu'une case à cocher si l'activité visée par le rapport comprend une composante cybernétique. Une étude a révélé une corrélation négative entre le taux de cybercriminalité et le nombre d'appels à la police, ce qui porte à croire que les régions où les services de police sont très occupés sont moins susceptibles d'enregistrer des incidents de cybercriminalité (Popham *et al.*, 2020).

Étant donné les différences de méthodologies utilisées pour mesurer la criminalité cyberfacilitée et la faiblesse du recueil des données dans certains États, il n'est souvent pas possible de comparer précisément l'évolution avec le temps ou de comparer utilement les statistiques entre les pays (Reep-van den Bergh et Junger, 2018; Caneppele et Aebi, 2019). De plus, l'estimation et le calcul précis des coûts de la criminalité se heurtent également à des difficultés méthodologiques lorsque les éléments en ligne et hors ligne se chevauchent (Levi, 2017). Audelà des difficultés de mesure, il est important d'examiner de manière critique l'origine et la validité des statistiques disponibles sur la cybercriminalité (Dupont, 2021). Les données sur la cybercriminalité recueillies et partagées par les entreprises privées servent souvent à promouvoir les services de cybersécurité de ces dernières et peuvent donc ne pas être fiables ou méthodologiquement rigoureuses en soi (Dupont, 2016a ; Caneppele et Aebi, 2019). Autrement dit, comme les entreprises de cybersécurité se concentrent principalement sur la cybercriminalité ciblant les entreprises et les gouvernements, on dispose de moins d'ensembles de données sur la cybercriminalité axée sur la société civile pour guider les initiatives de sécurité en ligne (Maschmeyer *et al.*, 2021).

On sait également que la cybercriminalité, crimes cyberfacilités compris, est sous-déclarée à l'échelle mondiale comme au Canada (Wanamaker, 2019; GRC, 2021b). Les gens peuvent percevoir ces types de crimes comme moins graves que d'autres, croire qu'il n'y aura pas de conséquences pour les délinquants ou ne pas être conscients du tout qu'un crime a été commis (Bidgoli et Grossklags, 2016). Une étude estime que les cybercrimes entièrement numériques et ceux comportant une composante cybernétique (c.-à-d. crimes hybrides) pourraient représenter entre un tiers et la moitié de tous les crimes commis dans les pays à hauts revenus, ce qui révèle une sous-déclaration massive de la cybercriminalité (Caneppele et Aebi, 2019). Les difficultés à déclarer et à mesurer la cybercriminalité ont conduit certains chercheurs à suggérer que l'augmentation des cybercrimes a contribué à un déclin apparent de la criminalité non

cybernétique signalée dans de nombreux pays depuis les années 1990 (Tcherni *et al.*, 2016; Caneppele et Aebi, 2019; Dupont, 2021). Autrement dit, la baisse des taux de criminalité peut être due, en partie, à l'émergence d'une cybercriminalité non détectée, à l'évolution d'une criminalité traditionnellement hors ligne vers une criminalité utilisant Internet ou à la migration vers des formes de cybercriminalité plus accessibles ou plus lucratives. Comme indiqué plus haut, les méfaits mentionnés dans ce rapport ne constituent pas tous des comportements criminels et sont aussi probablement en augmentation, mais les données relatives aux méfaits non criminels sont très limitées.

Les forces de l'ordre admettent les difficultés à mesurer et à signaler la cybercriminalité, et des outils de signalement plus détaillés et plus cohérents sont en cours d'élaboration au Canada. Statistique Canada a annoncé son intention d'employer le NACCC pour recueillir de manière cohérente des statistiques plus précises sur les incidents de cybercriminalité (Parker, 2021). Cette décision a pour but d'instaurer une terminologie uniforme entre les différents acteurs de la lutte à la cybercriminalité, tant au Canada qu'à l'étranger (StatCan, 2021c). Le NACCC a été approuvé par l'Association canadienne des chefs de police, qui a appuyé son utilisation dans toutes les forces de l'ordre municipaux, provinciaux ou territoriaux et fédéraux au Canada (Parker, 2021).

1.4 Structure du rapport

Le rapport répond au mandat en étudiant la sécurité numérique sous l'angle des droits de la personne

Pour répondre au mandat, le rapport explique tout d'abord les menaces actuelles et émergentes qui pèsent sur l'environnement en ligne et le lien entre ces menaces et les droits de la personne au Canada. Le chapitre 2 pose les bases de l'examen par le comité d'experts de la sécurité numérique en décrivant l'interaction entre la vie privée, la sécurité et les droits de la personne dans le domaine des données personnelles, de la surveillance et des libertés personnelles et relationnelles. Il se focalise en particulier sur l'individu plutôt que sur le collectif sociétal et décrit comment la vie privée, la sécurité et les droits de la personne sont traités dans les espaces numériques — et comment les atteintes à ces valeurs peuvent mener à des actes préjudiciables, voire criminels.

Les chapitres 3 et 4 examinent les façons dont les activités préjudiciables ou criminelles se sont adaptées pour intégrer les TIC. Le chapitre 3 décrit les préjudices qui sont directement attribuables aux technologies numériques. Si certains méfaits, tels que la diffusion de MAP et de contenu intime non consensuel, constituent des infractions criminelles, ils peuvent être difficiles à détecter et à contrer à cause de ces technologies. Mais d'autres actes abordés au

chapitre 3, comme certains cas de harcèlement en ligne, peuvent être préjudiciables, constituer de l'exploitation ou être autrement répréhensibles tout en étant légaux. Dans certains cas, il s'avère que la criminalisation n'est pas le moyen le plus efficace de lutter contre les dommages causés par les méfaits cyberfacilités.

Le chapitre 4 se penche sur les facilitateurs numériques de méfaits, notamment le Web invisible (*Deep Web*) et le Web clandestin (*Dark Web*), les cryptomonnaies et les platesformes de médias sociaux. Il examine également des services et des technologies qui n'ont peut-être pas été conçus dans le but de perpétrer ou de perpétuer des méfaits, mais qui sont utilisés pour — ou ont le potentiel de — créer des possibilités d'activités illégales et préjudiciables ainsi que le discours susceptible d'encourager les gens à s'engager dans des activités préjudiciables. Il se penche également sur les façons dont les platesformes numériques s'automodèrent, tout en manquant parfois de transparence, de responsabilisation et de cohérence dans ce domaine; dans certains cas, cela est dû à l'absence d'incitations, de pression du public ou de réglementation forte pour motiver des pratiques de modération souhaitables.

Les chapitres 5 et 6 traitent des problèmes et des possibilités qui ont émergé en matière de réglementation, de prévention, d'enquête, de poursuites et de lutte contre les crimes et les méfaits cyberfacilités. Le chapitre 5 décrit les approches réglementaires actuelles et émergentes au Canada et à l'étranger. Malgré les tentatives de dissuader, de protéger et de compenser par des moyens juridiques, la rapidité du développement technologique rend difficiles l'interprétation et l'application des lois sur les méfaits et les crimes cyberfacilités. Les décideurs politiques canadiens et étrangers réfléchissent à la manière dont le droit pourrait être réformé pour surmonter certains des défis que les TIC posent à la sécurité publique. Toutefois, la gouvernance étatique des espaces numériques se heurte à des difficultés lorsqu'il s'agit de trouver un équilibre entre la protection des victimes ou des survivants de cybercrimes et les droits et libertés constitutionnels, tels que la liberté d'expression et la vie privée.

Le chapitre 6 examine les difficultés rencontrées sur le terrain par les forces de l'ordre et par le système de justice pénale dans son ensemble pour enquêter sur les crimes cyberfacilités et engager des poursuites, et examine certaines pratiques émergentes qui peuvent aider à surmonter ces obstacles. Les déficits de compétences et l'insuffisance des ressources (y compris le manque de personnel) sont des obstacles majeurs aux enquêtes et aux poursuites relatives aux crimes cyberfacilités, de même que la faible coopération entre les organismes et les lacunes cruciales dans les données sur la fréquence et les répercussions des crimes cyberfacilités. Les défis découlant des obstacles à l'obtention de preuves numériques et du chiffrement sont étudiés, tout comme l'importance de ces outils

pour la protection de la sécurité publique. Il existe de nouvelles technologies pour aider les forces de l'ordre à surmonter tout un ensemble de difficultés, mais chacune s'accompagne d'éléments de réflexion éthiques qui lui sont propres, leur utilisation inappropriée pouvant entraîner une atteinte à la vie privée ou aux droits de la personne.

Le chapitre 7 conclut en exposant les réflexions du comité d'experts sur les questions clés soulevées dans ce rapport et souligne l'importance des approches responsables, centrées sur l'humain et prenant en considération les traumatismes pour lutter contre les crimes et les méfaits cyberfacilités.

2

Technologie numérique, vie privée et sécurité

Constatations du chapitre

- Les TIC sont présentes partout. De nombreux services essentiels comprennent une composante numérique, ce qui fait que tout le monde est numérique par défaut, même s'il est rarement en ligne. Ainsi, les questions touchant la protection de la vie privée et la sécurité numérique ont une incidence sur l'application de la *Charte canadienne des droits et libertés* et sur les droits de la personne de tout le monde au Canada.
- L'adoption des TIC peut amplifier l'interaction complexe entre la protection de la vie privée et la sécurité numérique, les libertés personnelles et associatives et la sécurité dans d'autres contextes en ligne. Toutefois, les outils de protection de la vie privée et de la sécurité ne s'opposent pas nécessairement et peuvent même se renforcer mutuellement.
- La multiplication des modes de recueil, d'utilisation et de communication des données des organismes publics et privés nécessite de réformer et de renforcer la législation qui protège les renseignements personnels et régit leur gestion au Canada.
- La protection de la vie privée dépend du contexte et est fondée sur des relations; les individus et les communautés doivent pouvoir prendre des décisions éclairées concernant leur vie privée en ligne.

Il est important d'examiner quels aspects du bien-être d'une personne sont menacés par les méfaits cyberfacilités. Ce chapitre pose les bases nécessaires pour répondre au mandat. Il met en contexte la relation entre les technologies numériques, la protection de la vie privée, la sécurité et les droits de la personne, et examine comment ces valeurs peuvent être violées non seulement lorsque nous sommes exposés à des méfaits cyberfacilités, mais aussi lorsque les outils et les mesures utilisés pour les prévenir sont appliqués de manière inappropriée.
Ce chapitre examine cette relation complexe, qui peut souvent créer un ensemble de facteurs à prendre en compte lors de la promulgation de lois, de politiques ou de règlements destinés à atténuer ou à prévenir les préjudices cyberfacilités.
Ce faisant, il aborde la relation potentiellement complémentaire entre la protection de la vie privée et la sécurité, explore la façon dont les intérêts individuels et collectifs en matière de protection de la vie privée et de sécurité sont liés aux droits de la personne et décrit certaines des manières dont la technologie influence la compréhension contemporaine de ces concepts par la société.

Le chapitre commence par présenter la vie privée comme un droit de la personne, qui est contextuel et défini par le contrôle et le flux de données et de renseignements relatifs aux individus et à leur communauté. Il lie ensuite la protection de la vie privée à la sécurité, en soulignant comment la protection de la vie privée et la sécurité des données peuvent se renforcer mutuellement. Enfin, ces concepts sont utilisés pour présenter certaines des difficultés générales rencontrées dans la conception et la mise en application de la réglementation sur la vie privée et sur la sécurité, comme le suivi ou l'anticipation des changements technologiques, le contrôle du respect de la vie privée et de la sécurité des utilisateurs par les entreprises et les entités privées (et l'imputation à ces dernières de la responsabilité des abus de confiance) et la coopération au-delà des frontières en matière de réglementation et d'application.

2.1 Vie privée, droits de la personne et sécurité publique numérique

2.1.1 Fusion des mondes numérique et physique

Les capacités Internet se développent rapidement et doivent être considérées comme une extension du monde physique

Les technologies numériques sont présentes dans presque tous les aspects de la vie moderne. La santé, la famille, les finances, l'éducation et l'amour — pour n'en citer que quelques-uns — sont tous concernés par les espaces numériques en constante évolution et s'y adaptent. La connectivité est de plus en plus nécessaire pour accéder à des services essentiels comme l'éducation et les soins de santé, participer au marché du travail, faire des achats et maintenir des liens sociaux (CAC, 2021; StatCan, 2021a). Autrefois, le monde numérique se limitait à des forums de discussion anonymes et au partage de données de base, et il était largement séparé de la vie quotidienne. Aujourd'hui, il est pratiquement indissociable du monde physique, à tel point que la distinction n'est plus qu'une relique du passé (Dubois et Martin-Bariteau, 2020a), ce qui fait que tout le monde peut être victime des types de crimes et de méfaits cyberfacilités abordés dans ce rapport.

Les choix de conception faits à la naissance d'Internet ont une incidence énorme sur la vie moderne et sur la nature des méfaits en ligne

Internet a été fondé sur les principes de la libre circulation de l'information et de la décentralisation du contrôle (Krasodomski-Jones, 2021), mais ces principes ont eu des conséquences imprévues. Comme l'a écrit son inventeur, Tim Berners-Lee, à l'occasion du 30e anniversaire de son introduction :

> *J'avais espéré que 30 ans après sa création, nous utiliserions le Web avant tout pour servir l'humanité [...] Mais la réalité est bien plus complexe. Les communautés sont déchirées par les préjugés, la haine et la désinformation colportés en ligne. Les escrocs utilisent le Web pour voler des identités, les harceleurs s'en servent pour harceler et intimider leurs victimes et les acteurs malfaisants sapent la démocratie en utilisant des tactiques numériques astucieuses. [traduction libre]*
>
> Berners-Lee (2019)

Grâce aux technologies de l'information et des communications (TIC), de nombreuses sociétés contemporaines sont devenues sociales et connectées d'une manière qui a considérablement modifié la façon dont leurs membres perçoivent la protection de la vie privée et la sécurité. La connectivité accrue a également révélé que la signification et l'importance de la protection de la vie privée et de la sécurité varient — souvent en fonction des valeurs personnelles et sociétales (Bambauer, 2013). Par exemple, dans la société canadienne, la protection de la vie privée et la sécurité sont souvent présentées comme opposées l'une à l'autre, dans la mesure où la sécurité exige une surveillance intrusive des individus, tandis que la protection des données et de la vie privée demande de limiter l'accès aux données. Ce chapitre décrit plutôt les deux concepts comme souvent complémentaires et note que l'affaiblissement du respect de la vie privée au profit de la sécurité peut être contreproductif.

En raison de la nature dynamique de ces questions, le débat entourant la définition de la *protection de la vie privée* et ses limites peut créer des divergences entre les chercheurs (p. ex. Etzioni, 2005; Bailey, 2008; Solove, 2008; Kerr et Barrigar, 2012; Krishnamurthy *et al.*, 2021), les législateurs (sections 5.2 et 5.4) et les tribunaux (p. ex. CSC, 2014a, 2016a, 2021). La gestion de la vie privée et de la sécurité numérique est de plus en plus compliquée, car les gens vivent de plus en plus leur vie en ligne. La quantité et les types de renseignements en ligne partagés sur une personne donnée ont rapidement augmenté, sont devenus plus difficiles à gérer et peuvent être très sensibles. Par conséquent, tout nouveau dispositif de sécurité doit être évalué avec soin, en sachant que les avantages en matière de vie privée peuvent être obtenus au détriment des libertés, de l'anonymat ou de la sécurité dans d'autres domaines (Landau, 2011; Hartzog, 2018). En outre, alors que des entités internationales (y compris des entreprises privées) se sont mises à recueillir des quantités massives de données d'utilisateurs, ces infractions calculées doivent être considérées dans un contexte mondial en rapide évolution (Hartzog, 2018; Farrell et Newman, 2019).

2.1.2 Comprendre la vie privée

La vie privée est un droit individuel et une valeur sociale collective

Le concept de vie privée englobe souvent plusieurs droits et libertés, tels que la liberté de pensée, la liberté de choix concernant son corps, la liberté de toute surveillance et la liberté de contrôler les renseignements à propos de soi (Solove, 2002, 2015; Cockfield, 2007; Bernier, 2012). La conception de ce qu'est la vie privée est également dynamique, enracinée dans l'histoire du pays et a évolué au fil du temps (Hartzog, 2018). La vie privée à l'échelle individuelle (en particulier par rapport aux entités non gouvernementales) est sans doute un principe relativement nouveau, qui nécessite davantage de protections, car la technologie crée de multiples occasions de la compromettre (Becker, 2019). Il convient de noter que si ce chapitre se concentre sur la manière avec laquelle les technologies numériques peuvent influencer la façon dont un individu vit sa vie privée et sa sécurité, il existe également des dimensions collectives à la vie privée et à la sécurité qui peuvent être prises en compte (Thompson et Lyon, 2021).

Les débats contemporains sur la vie privée se concentrent sur la compréhension des droits individuels, tels que « le droit des individus à avoir *leur propre domaine*, séparé du public » [traduction libre] (Becker, 2019). Il est important de noter que la vie privée est un droit humain reconnu (Scassa, 2020), qui « permet la jouissance d'autres droits, comme développer et exprimer librement sa personnalité, son identité et ses croyances, et être en capacité de participer à la vie politique, économique, sociale et culturelle » (HCDH, 2021). La vie privée peut également être comprise comme une valeur sociale collective qui rend possibles « les valeurs démocratiques essentielles à la promotion de la sécurité à long terme » [traduction libre] (Cockfield, 2007). En 2021, la Cour suprême du Canada a statué dans l'affaire *Sherman Estate c. Donovan* que « [b]ien que la vie privée d'une personne soit d'une importance primordiale pour celle-ci, la protection de la vie privée est également dans l'intérêt de la société dans son ensemble. La vie privée ne saurait donc être rejetée en tant que simple préoccupation personnelle : il y a chevauchement entre certaines préoccupations personnelles relatives à la vie privée et les intérêts du public » (CSC, 2021). La Cour poursuit en concédant que « [l]a vie privée est une notion complexe et contextuelle, de sorte qu'il est difficile pour les tribunaux de la mesurer » (CSC, 2021). Dans certains cas, il peut être déterminé que la sécurité d'un groupe sociétal peut supplanter les considérations de vie privée individuelle ou collective. Par exemple, la collecte massive de données et la surveillance de masse peuvent être utiles pour la sécurité nationale, mais elles peuvent avoir des répercussions négatives sur le bien public si elles compromettent le genre de vie privée collective attendue dans un État démocratique (Thompson et Lyon, 2021). Cette discussion dépasse cependant la portée du présent rapport.

2.1.3 Protection de la vie privée et sécurité des données

La sécurité des données peut être considérée comme un droit humain fondamental ou comme le résultat du droit à la vie privée

Les limites de la vie privée peuvent être fluides ou peu claires; parfois, la loi détermine que la vie privée individuelle doit être soumise à des limitations raisonnables au bénéfice d'autres intérêts, tels que le besoin de certaines formes de sécurité (Cockfield, 2007; Kerr et McGill, 2007; Chandler, 2009; Aquilina, 2010). Pour prendre des décisions éclairées sur la protection de la vie privée en ligne, il faut toutefois comprendre comment celle-ci est liée aux données personnelles.

La conception que les gens ont de la vie privée et de la sécurité n'est pas fixe dans le temps et identique d'un pays à l'autre. Les gouvernements et les organismes ont leur propre point de vue sur la vie privée, la sécurité et la manière de les protéger, et ils ont dû s'adapter à mesure de l'évolution des TIC pour faire face au volume de données personnelles et publiques accessibles (et, dans les faits, recueillies) en ligne. Par exemple, le Canada et l'Union européenne (UE) reconnaissent tous deux que la vie privée est un droit humain, mais diffèrent dans la manière dont il protège la sécurité des données. L'UE considère la vie privée et la protection des données (qui inclut la sécurité des données) comme des droits distincts, mais qui se chevauchent; cette approche se reflète dans l'article 8 de la *Charte des droits fondamentaux de l'Union européenne* et est comparable à la protection de la vie privée décrite dans la Déclaration universelle des droits de l'homme et dans le Pacte international relatif aux droits civils et politiques (CPVP, 2021a) (encadré 2.1). Dans un rapport annuel concernant la période 2020–2021, le Commissariat à la protection de la vie privée du Canada indique que l'approche de l'UE a eu une influence importante sur le Canada (CPVP, 2021a); cette philosophie peut teinter l'application d'outils tels que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) aux cas de protection des données, mais la protection des données en tant que droit de la personne n'est pas une caractéristique explicite de la législation canadienne (Bygrave, 2010).

La vie privée est contextuelle, relationnelle et inclut le partage consensuel des données

La collecte de données personnelles par des entités privées et publiques a conduit à décrire la vie privée et la sécurité comme des constructions sociales capables de s'adapter, contextuellement, aux relations des gens avec d'autres entités (Steeves, 2009). La protection de la vie privée nécessite donc de comprendre les interactions entre ceux qui recherchent ou respectent la vie privée — une relation qui, selon Steeves (2009), est en constante évolution et peut être négociée. Les normes relatives à la vie privée nous permettent de contrôler l'identité sociale — le soi qui

est présenté au monde —, mais les avancées technologiques, telles que l'analyse des mégadonnées, mettent en péril ce contrôle (Austin, 2012) (encadré 2.1).

Encadré 2.1 Contrôle des données personnelles et droit à l'autodétermination

Les politiques fondées sur les données probantes s'appuient sur les renseignements, mais les renseignements recueillis (et, fait notable, ceux qui ne le sont pas) peuvent influencer de manière disproportionnée la façon dont certaines communautés sont perçues par l'État. Par exemple, Walter *et al.* (2020) expliquent que « pour les peuples autochtones, la tranche de nos réalités sociales et culturelles représentée dans les données recueillies à notre sujet se limite aux aspects qui intéressent l'État-nation » [traduction libre]. Ils ajoutent que « la tranche particulière et limitée de la vie autochtone qui intéresse l'État a une forte influence sur le comment et le pourquoi les politiques autochtones continuent de dérailler dangereusement. Ces données forment le système qui soutient la longue histoire de plans politiques ratés qui tentent de «refaire les sociétés autochtones» » [traduction libre]. La Déclaration des Nations Unies sur les droits des peuples autochtones, un instrument international de défense des droits de la personne officiellement ratifié par le Canada en 2016 et qui est devenu loi en 2021, est conforme au mouvement pour la souveraineté des données autochtones, qui cherche à donner aux communautés autochtones la capacité de façonner certaines décisions politiques à leur avantage — un principe de protection de la vie privée qui souligne le pouvoir de façonnement des communautés et de contrôle des données recueillies à leur sujet (ONU, 2007; Kukutai et Taylor, 2016; Duncanson *et al.*, 2021; Lukings et Lashkari, 2022a).

En tant que signataire de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques, le Canada a convenu que la protection juridique de la vie privée est un droit de la personne (ONU, 1948, 1966; GC, 2019a). Cette protection peut être examinée dans un contexte personnel (p. ex. pour donner la capacité de développer et d'exprimer sa personnalité, son identité et ses croyances sans interférence) ou dans un contexte social (p. ex. protéger une structure sociétale qui valorise ces libertés individuelles). Dans un cas comme dans l'autre, et étant donné l'évolution constante des modes de recueil numérique des données et renseignements personnels, l'interprétation de ces droits et la fourniture de ces protections constituent un objectif en constante évolution (Kukutai et Taylor, 2016; Walter *et al.*, 2020; Duncanson *et al.*, 2021).

Le concept d'*intégrité contextuelle* élaboré par Nissenbaum (2010) décrit plus en détail la relation entre vie privée et société, tout en tenant compte des structures et des valeurs sociales. Le contexte social d'une personne (déterminé par la politique, l'éducation, les soins de santé et autres éléments) peut définir les attentes en matière de protection de la vie privée, qui sont de plus influencées par des éléments géographiques, historiques et culturels. L'auteur note que, lorsqu'on envisage la protection de la vie privée à l'ère numérique, « ce dont les gens se soucient le plus n'est pas simplement de *restreindre* le flux d'informations, mais de s'assurer qu'il circule de *manière appropriée* » [traduction libre] (Nissenbaum, 2010). Il ne s'agit pas de renoncer à sa vie privée, mais plutôt d'avoir des attentes raisonnables en ce qui concerne sa protection.

Résumant plusieurs théoriciens de la protection de la vie privée, Bambauer (2013) écrit que la protection de la vie privée à l'ère numérique « ne consiste plus en une division binaire entre données révélées et données dissimulées. Il s'agit de revendications concurrentes en matière d'information » [traduction libre]. Autrement dit, la question est de savoir quels acteurs devraient être autorisés à utiliser les données, et pourquoi ces acteurs (et pas d'autres, en particulier dans les communautés racisées et marginalisées) se voient accorder ce pouvoir (Bambauer, 2013; Walter *et al.*, 2020). La question de la vie privée à l'ère numérique ne se limite pas au contrôle du recueil de renseignements; elle concerne également « le processus par lequel les renseignements sont recueillis, traités et utilisés — un processus qui est lui-même hors de contrôle » [traduction libre] (Solove, 2002). Le problème de la protection de la vie privée réside dans l'agrégation des données, l'absence de réglementation notable de ces données et le contrôle sur la façon dont les données d'une personne sont utilisées (Solove, 2002).

Waldman (2018) développe ce concept dans le contexte de la confidentialité des renseignements, qui « ne consiste pas à exclure les autres, mais plutôt à réguler le flux de renseignements vers certains, à le restreindre de certains et à l'ouvrir aux autres » [traduction libre]. S'appuyant sur le travail de Nissenbaum, l'auteur note l'importance de la confiance dans la mise en pratique de la communication entre les individus, et entre les utilisateurs et leurs platesformes, et suggère que la confiance dans un système de protection de la vie privée doit être « administrable » et « capable d'être appliquée par les avocats et les juges dans des cas réels afin de répondre à des questions réelles de confidentialité des renseignements » [traduction libre]. Dans ce contexte, protéger la vie privée consiste à créer une relation permettant la communication en toute tranquillité (Waldman, 2018). En ce sens, la sécurisation des données et des renseignements personnels peut être vue comme un élément de la protection de la vie privée.

La notion de protection de la vie privée change pour les victimes et survivants de méfaits qui ciblaient cette vie privée

La vie privée est nuancée et contextuelle, et prend une dimension différente une fois qu'elle a été attaquée. Les victimes et les survivants de méfaits tels que le partage non consensuel d'images intimes, de matériel d'abus pédosexuels (MAP) et d'autres formes d'abus sont contraints de tenir compte de critères de protection de la vie privée différents de ceux des personnes dont la vie privée n'a pas encore été compromise. En particulier, le recouvrement de sa vie privée peut devenir une priorité absolue pour les personnes lésées, même s'il est difficile, voire impossible, d'y parvenir. Cet aspect de la protection de la vie privée est examiné plus en détail au chapitre 3, notamment dans le contexte de la suppression et de la désindexation des renseignements portant atteinte à la vie privée et d'autres méthodes curatives reposant sur le traumatisme.

2.2 La nature de la sécurité à l'ère numérique

2.2.1 Protection de la vie privée et sécurité : une fausse dichotomie

La sécurité numérique est parfois assurée au détriment du respect de la vie privée, des libertés individuelles et associatives et de la sécurité dans d'autres domaines

Les nouvelles technologies numériques s'accompagnent de nouvelles menaces, et l'infrastructure de sécurité doit elle aussi évoluer à mesure que les capacités sur le Web se développent. Le téléphone d'un individu peut contenir une foule de données, notamment des courriels personnels, des renseignements financiers, des identifiants de connexion et l'accès à des comptes professionnels (Bohannon, 2018). En raison de la sensibilité d'une grande partie de ces données, celles-ci doivent être protégées contre le piratage en ligne, mais la mobilité des téléphones intelligents en fait également des cibles faciles pour les voleurs. C'est pourquoi les développeurs s'efforcent de rendre ces appareils impénétrables, afin de réduire le risque de compromission des données personnelles ou d'identification en cas de vol. Cependant, ce genre de sécurité des données pose problème aux forces de l'ordre lorsqu'elle rend inaccessibles des preuves potentielles (Landau, 2017) (section 6.3). Le comité d'experts conclut donc que la *sécurité* peut être envisagée en tant que pouvoir — qui peut faire quoi, et à quelles conditions, avec un dispositif, un système ou un élément d'infrastructure particulier. Les technologies visant à renforcer la sécurité déplacent ce pouvoir; il est donc essentiel que les changements découlant de l'adoption de nouvelles technologies soient étudiés sur le plan de l'acceptabilité sociale et de l'éthique, et en tenant compte du fait que les individus peuvent avoir une vision différente de la vie privée et de la sécurité.

2.2.2 Recueil massif de données et surveillance

La surveillance et le recueil massif de données peuvent compromettre la vie privée et la sécurité

La technologie procure également une capacité sans précédent de recueil, de transfert et de stockage des données. Cette capacité donne aux institutions de tous types (p. ex. sécurité, entreprise, politique) le pouvoir de surveiller et de profiler des individus ou des groupes spécifiques, souvent à l'insu de ceux-ci (Alexander, 2015; Becker, 2019). Le recueil de données à des fins de surveillance — par les forces de l'ordre ou par des organismes gouvernementaux — est inquiétant en ce qui concerne la vie privée et les droits de la personne, en particulier lorsque le processus est peu transparent ou peu contrôlé (Robertson *et al.*, 2020).

Toutefois, ce n'est pas la seule préoccupation touchant le recueil de données en ligne. Outre la surveillance, le profilage basé sur les données a la capacité d'influencer la prise de décision individuelle — par exemple, par le biais de la publicité ciblée, qui alimente en partie l'industrie du courtage de données, d'une valeur estimée à 200 milliards de dollars américains, laquelle transforme les données personnelles en marchandises (Harris, 2017; Becker, 2019; McClelland, 2021). Dans le même temps, le recueil massif et l'agrégation des données des citoyens posent des risques pour la sécurité, même si l'entreprise responsable adhère à des pratiques de sécurité acceptables ou conformes aux normes du secteur. Les atteintes à la sécurité d'entreprise (p. ex. au moyen de logiciels malveillants, de l'espionnage ou de rançongiciels) constituent non seulement une attaque financière contre une entreprise, mais compromettent également la vie privée et la sécurité de ses clients (Centre canadien pour la cybersécurité, 2021b; La Presse Canadienne, 2021). Le Centre canadien pour la cybersécurité (2021b) explique que « [l]es opérateurs de rançongiciels utilisent de plus en plus la tactique consistant à rendre publiques les données d'une victime si celle-ci ne paye pas la rançon ». Bien que le nombre de ces attaques soit difficile à mesurer, le Centre canadien pour la cybersécurité (2022a) affirme également que « [l]es rançongiciels ont presque assurément une incidence plus importante sur les organisations canadiennes aujourd'hui [en 2022] qu'en 2020 ». Par ailleurs, les données sont parfois volées et rendues publiques par des pirates, puis utilisées par d'autres pour faire chanter les victimes ou leur extorquer de l'argent, comme ce fut le cas en 2015 lorsque le service de rencontres amoureuses Ashley Madison a été piraté (Doffman, 2020). Dans un autre cas, 520 patients du Health Service Executive d'Irlande (le système de santé irlandais) ont été victimes d'une fuite de données sur le Web en 2021 à la suite d'une attaque par rançongiciel, qui a causé une perturbation importante des services vitaux aux patients (Gallagher, 2021; McNamee, 2021) (récit 1).

Récit 1 Rançongiciels et dommages collatéraux en Irlande, 2021

Les attaques par rançongiciels visent souvent des entreprises et des organisations ayant accès à de grosses sommes d'argent, mais les perturbations et les préjudices qui en résultent peuvent également être ressentis par des particuliers. En 2021, Conti, un groupe de rançongiciels basé en Russie, a ciblé le système de santé irlandais, parvenant à chiffrer des données importantes qui ont obligé les services à annuler jusqu'à 80 % de leurs rendez-vous. L'attaque a coupé l'accès à des données et à des appareils importants sur l'ensemble du réseau du système, ce qui a eu des répercussions sur presque tous les éléments de ce système et a obligé le personnel à trouver des moyens de s'adapter.

L'un des rendez-vous annulés concernait Donna-Marie Cullen qui, le jour de l'attaque, était sur le point de subir une séance de radiothérapie contre une forme agressive et mortelle de cancer du cerveau. Heureusement, une autre unité d'oncologie a pu déconnecter ses appareils du système et, après plusieurs jours de travail, a réussi à modifier le plan de soins de M^{me} Cullen pour la nouvelle machine et à reprendre le traitement. Bien que la plupart des services aient été rétablis au bout d'une semaine environ (une fois la clé de chiffrement obtenue), les perturbations ont persisté longtemps après, en particulier dans les unités d'oncologie et dans d'autres services fortement tributaires du traitement des données et des techniques de calcul.

(McNamee, 2021)

2.2.3 Droits de la personne et outils reposant sur des algorithmes

Les données utilisées hors contexte peuvent poser des problèmes pour la vie privée, les droits de la personne et les libertés civiles

Des systèmes et services prédictifs *et al*gorithmiques ont été conçus dans le but d'utiliser de grands ensembles de données afin de détecter les comportements illicites ou d'y répondre (Thompson et Lyon, 2021). Cependant, « sans intervention humaine dans l'analyse des données, la probabilité de succès de l'utilisation des mégadonnées pour le renseignement de sécurité et la surveillance demeurera mince. L'accent mis sur les algorithmes et sur les machines détourne précisément l'attention des questions cruciales de contexte » [traduction libre] (Thompson et Lyon, 2021). Par conséquent, on ne peut pleinement tirer profit de la valeur des

mégadonnées que grâce à l'intelligence humaine appropriée nécessaire pour les contextualiser (Van Puyvelde *et al.*, 2017; Thompson et Lyon, 2021). Cela ne signifie pas pour autant que l'intervention humaine suffit à atténuer les biais (Završnik, 2020) ni qu'elle s'attaque aux biais inconscients des gens. Chaque étape d'un processus décisionnel algorithmique peut introduire un biais, y compris le recueil des données, leur préparation (c.-à-d. l'exclusion ou l'inclusion de données), la conception de l'algorithme et sa mise en œuvre. Dans un système aussi complexe, il peut être impossible de déterminer à quel endroit de la boucle la prise de décision humaine pourrait être utile, si tant est qu'elle puisse l'être (Završnik, 2020).

Aussi prometteuses que semblent être les techniques de mégadonnées, elles dépendent des données d'entrée, qui peuvent être biaisées, de qualité douteuse ou intentionnellement compromises (Robertson *et al.*, 2020; Bull, 2021). Étant donné l'importance de certains des problèmes que ces techniques ont permis de résoudre (p. ex. les biais dans le maintien de l'ordre), les incertitudes concernant la façon dont les algorithmes de mégadonnées produisent des résultats restent au centre de nombreuses recherches (Ridgeway, 2018; Robertson *et al.*, 2020) et ont conduit à des appels aux gouvernements pour qu'ils restreignent leur utilisation dans le cadre de l'application de la loi, de l'immigration et d'autres domaines touchant la sécurité (Robertson *et al.*, 2020). Fait important, ce n'est pas seulement le climat politique et sociétal dans lequel ces technologies se répandent qui détermine la manière dont elles vont faire avancer ou entraver les droits de la personne, la protection de la vie privée et la sécurité, mais aussi leur conception intrinsèque (Winner, 1980; Starr, 2005).

Ce qui peut être considéré comme des limites acceptables à la vie privée et à la surveillance est contextuel et évolutif

Un point essentiel régissant la sécurité publique numérique est de savoir dans quelle mesure les droits de la personne, notamment le droit à la vie privée, peuvent ou doivent être supplantés par les besoins de sécurité. La réponse à cette question n'est pas facile, car elle dépend de plusieurs facteurs, qui peuvent inclure les besoins de sécurité personnels, l'idéologie, la position sociale ou le contexte culturel et historique (Bellman *et al.*, 2004; Nordal, 2013; Igo, 2018). Bien que divers outils technologiques soient déjà utilisés pour la surveillance, les enquêtes et les poursuites relatives aux crimes, le débat se poursuit sur les limites de leur utilisation lorsque celle-ci entre en conflit avec le droit à la vie privée, le droit d'association, le droit religieux ou d'autres droits protégés par la Charte (Lucock et Black, 2009; Robertson *et al.*, 2020). Par exemple, quelle doit être l'efficacité d'un outil technologique pour justifier son utilisation, sans parler de sa simple conception? Par ailleurs, l'efficacité et la facilité d'utilisation d'une technique peuvent-elles conduire à des pratiques excessivement invasives? La détection

proactive des pourriels et de l'hameçonnage par les services de courrier électronique, par exemple, fonctionne depuis de nombreuses années dans un souci minimal de respect de la vie privée. Cela dit, le système automatisé de filtrage du MAP proposé par Apple en 2021 pour analyser les photos sur les iPhones et dans iCloud a fait craindre qu'il puisse nuire au chiffrement de bout en bout d'Apple (Porter, 2021).

Un autre élément de réflexion concernant l'adoption de nouveaux outils numériques est leur comparaison avec leurs équivalents analogiques. Par exemple, l'amélioration des technologies numériques a radicalement modifié les capacités de surveillance des forces de l'ordre. Bankston et Soltani (2014) estiment que le coût du suivi d'un suspect par une poursuite secrète classique est presque 30 fois plus élevé que celui de son suivi avec un dispositif GPS. Si le suivi s'effectue au moyen d'un téléphone intelligent, la poursuite secrète est alors plus de 50 fois plus coûteuse. Si les progrès technologiques ont permis aux forces de l'ordre de suivre les suspects plus facilement et plus efficacement, ils « constituent une menace pour la vie privée en permettant une surveillance d'une ampleur qui, dans le passé, aurait été d'un coût prohibitif » [traduction libre] (Posner, 2007). De plus, dans quelle mesure les forces de l'ordre doivent-elles être tenues responsables lorsqu'elles utilisent un outil technologique particulier pour surveiller et contrôler? Dans quel but et pour quelle durée la conservation des données personnelles doit-elle être autorisée? Les gens sont-ils capables de déterminer un degré de sécurité acceptable pour eux-mêmes, qui satisfasse leur besoin de protection de leur vie privée et de sécurité en ligne, tout en protégeant leurs libertés civiles (Van Puyvelde *et al.*, 2017; Ferguson *et al.*, 2020). Il ne s'agit pas d'interrogations philosophiques, mais de préoccupations contemporaines et pratiques au sujet de l'application de la loi, qui sont étroitement liées aux contestations sur la mesure appropriée dans laquelle l'État peut exercer son pouvoir pour s'immiscer dans la vie privée et publique.

2.3 Réglementation dans le contexte de la protection de la vie privée, de la sécurité et des droits de la personne

2.3.1 La protection de la vie privée est une préoccupation nationale

Malgré les outils de gouvernance actuels, de nombreuses personnes au Canada sont préoccupées par la protection de la vie privée

La protection de la vie privée est un sujet de préoccupation pour de nombreuses personnes au Canada, malgré les réglementations en vigueur. Par exemple, un

sondage réalisé en 2018–2019 par le Commissariat à la protection de la vie privée a révélé que 92 % des répondants étaient plus ou moins préoccupés par la protection de leur vie privée, comparativement à 88 % en 2012; fait notable, le nombre de répondants qui se disaient « extrêmement préoccupés » est passé de 25 % en 2012 à 37 % en 2018 (CPVP, 2019a). D'autres encore se demandent si l'on peut compter sur le gouvernement lui-même pour protéger le droit à la vie privée, en particulier lorsque les appareils de sécurité gouvernementaux peuvent bénéficier des activités de surveillance grâce, par exemple, à un accès plus aisé à de gros volumes de renseignements jugés nécessaires pour certains buts, comme la lutte contre la criminalité ou le terrorisme (Alexander, 2015; Talbot, 2021).

2.3.2 Réglementation de la vie privée au Canada

Au Canada, la protection de la vie privée est réglementée par plusieurs ordres de gouvernement, selon des philosophies qui diffèrent d'une province ou d'un territoire à l'autre

Au Canada, le droit à la vie privée est protégé, entre autres, par l'article 8 de la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels* et la LPRPDE (GC, 1982, 1985, 2000a, 2020a; CPVP, 2019b) (section 5.1). En outre, chaque province et territoire peut régir la protection de la vie privée au moyen de ses propres lois applicables au secteur public et privé, ainsi que par la common law ou le droit civil (CPVP, 2018; GC, 2021g) (chapitre 5). Bien qu'il puisse être utile d'envisager la protection de la vie privée et la sécurité des données dans le cadre des droits de la personne, une grande partie du recueil de données et de la surveillance à grande échelle est effectuée par des entreprises privées et des platesformes Web, qui ne sont pas liées par des textes tels que la Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits civils et politiques, mais plutôt par la législation sur la protection de la vie privée (qui, pour le Canada, comprend la LPRPDE) (GC, 2000a, 2020a; Hartzog, 2018; CPVP, 2019b). Malgré ces lois, l'Assemblée citoyenne canadienne sur l'expression démocratique s'inquiète du fait que le droit de *ne pas* être soumis à une surveillance sans raison valable n'a pas été adéquatement pris en compte dans la conception des platesformes numériques (CCADE, 2021).

La LPRPDE réglemente les relations entre les entreprises et les particuliers et n'a pas été conçue pour protéger la vie privée en tant que droit de la personne

La LPRPDE, qui a été adoptée en 2000, a été élaborée à une époque où 51 % des ménages canadiens comptaient au moins un membre utilisant régulièrement Internet (StatCan, 2001), et avant la popularisation des médias sociaux et du marketing en ligne. Au cours des années qui ont suivi son adoption, le Comité

permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) de la Chambre des communes a tenu des audiences sur la façon dont les lois sur la protection de la vie privée tiennent compte d'une variété de progrès sociaux et technologiques nouveaux, émergents et autrement difficiles à prévoir. Selon Scassa (2020), la LPRPDE repose trop fortement sur le consentement individuel, qui est souvent présenté dans un langage compliqué et demandé assez fréquemment pour que de nombreux utilisateurs soient incapables de donner un véritable consentement éclairé. Les défenseurs de la vie privée ont également fait valoir que la LPRPDE n'est pas suffisamment appliquée (section 5.1.4) et que de manière générale, elle ne tient pas compte des dimensions collectives de la protection de la vie privée (Scassa, 2020).

Les Principes directeurs relatifs aux entreprises et aux droits de l'homme (UNGP) des Nations Unies cherchent à contribuer à la résolution de ce problème en garantissant que les activités des entreprises n'interfèrent pas avec les droits de la personne (CDH, 2011b). L'UNGP a fait l'objet de critiques pour ne pas tenir les entreprises juridiquement responsables, et « pour fixer la barre plus bas que les normes internationales en matière de droits de la personne dans certains domaines, comme la garantie du droit à réparation d'une victime » [traduction libre] (Albin-Lackey, 2013). Pour faire face à la question des méfaits cyberfacilités, les entreprises privées sont souvent soumises à des exigences de la part des gouvernements, telles que le signalement aux forces de l'ordre des activités préjudiciables ou illégales se déroulant sur leur plateforme ou le retrait dans les plus brefs délais du contenu préjudiciable (chapitre 5). Ces exigences compliquent les relations entre le gouvernement et les entreprises privées (Ferguson, 2017; Landau, 2017). La responsabilité des platesformes pose également problème lorsque celles-ci sont transnationales et nécessitent des accords négociés entre gouvernements étrangers et entreprises privées (encadré 2.2).

Encadré 2.2 Les entreprises privées comme nouveaux régulateurs

D'énormes quantités de données personnelles sont recueillies par des entreprises privées, dont beaucoup mènent des activités à l'échelle internationale. Assurer la sécurité des données nécessite le travail et la coopération des gouvernements et de leurs organismes de réglementation, des forces de l'ordre, des entreprises et des citoyens. Certains affirment que la réglementation qui s'applique aux grandes entreprises numériques, telles que Meta, la société mère de Facebook, et Twitter, « est plutôt de l'ordre de la gouvernance privée et de l'autorégulation » [traduction libre]. Dans de nombreux cas, les platesformes élaborent leurs propres mécanismes, qui s'apparentent à une forme de gouvernance étatique, qui comprennent notamment un organe directeur central, des politiques et des règles fondées sur des valeurs démocratiques pouvant être utilisées pour juger les comportements inappropriés sur la plateforme et des modes de modification et de mise à jour de ces règles. On a aussi suggéré que le terme *gouvernance* est en effet la meilleure façon de traduire l'idée du pouvoir qu'ont ces platesformes de façonner les lois et les règlements internationaux, et on les a surnommées les *nouveaux régulateurs* de l'ère numérique. Cette vision d'Internet diffère de la vision initiale, soit celle d'une démocratie en ligne décentralisée. Aujourd'hui, ces nouveaux régulateurs forment une couche supplémentaire de gouvernance, qui se situe entre l'État et les citoyens. Il s'agit d'une transformation sans précédent du pouvoir mondial, qui a d'énormes répercussions sur la sécurité numérique des individus au Canada.

(Klonick, 2018)

Comme la LPRPDE, la *Loi sur la protection des renseignements personnels* fédérale, qui est appliquée par le Commissaire à la protection de la vie privée du Canada, fixe des règles sur la façon dont le gouvernement traite les données et la vie privée, et a fait l'objet d'une révision ces dernières années, sous l'influence du *Règlement général sur la protection des données* (RGPD) de l'UE (Scassa, 2020). Therrien (2021a) et d'autres ont suggéré que la *Loi sur la concurrence* canadienne soit passée en revue et réformée en même temps que la *Loi sur la protection des renseignements personnels* afin de mieux s'attaquer aux répercussions du *capitalisme de plateforme et de surveillance* sur la sécurité des données et la vie privée des utilisateurs (Qarri, 2022). L'argument rappelle essentiellement l'effet de la concurrence sur les prix à la consommation; lorsque la domination du marché

(ou le monopole) réduit la concurrence, les consommateurs n'ont que peu ou pas d'autres solutions appropriées, ce qui permet d'augmenter les prix pour un produit ou un service potentiellement inférieur (Therrien, 2021a; Qarri, 2022). Dans le cas des platesformes en ligne qui recueillent et monétisent les données des utilisateurs, un produit ou un service inférieur pourrait inclure des pratiques de protection de la vie privée de moindre qualité; fait notable, les deux effets peuvent agir simultanément (Qarri, 2022). L'article 20 du RGPD exige la portabilité des données, et des contrôles supplémentaires ont été proposés, notamment l'interopérabilité des platesformes (p. ex. la possibilité d'envoyer directement des messages entre les différentes platesformes) afin que les utilisateurs ne soient pas prisonniers de services spécifiques pour communiquer avec leurs réseaux personnels (De Hert *et al.*; OCDE, 2021). Les partisans de cette approche affirment que ces caractéristiques peuvent favoriser la concurrence et permettre aux utilisateurs d'influer sur la manière dont leur vie privée et la sécurité de leurs données sont traitées, grâce à la pression du marché (Qarri, 2022) (section 5.2). Leurs opposants dans le débat sur l'interopérabilité soulignent toutefois le succès d'Apple en tant qu'entreprise de matériel et de logiciels de bout en bout, ainsi que les nouveaux risques pour la vie privée aux frontières entre les différentes platesformes (Graves, 2021).

2.3.3 Difficultés posées par la réglementation numérique

La vitesse à laquelle les technologies évoluent et sont adoptées rend difficile la réglementation des espaces numériques

En raison de la rapidité des changements technologiques, les questions de la protection de la vie privée et de sécurité évoluent constamment. Les forces de l'ordre, par exemple, peuvent être contraintes d'interpréter la loi de manière « créative » pour justifier l'adoption de certaines techniques ou outils technologiques, ou d'accéder à des catégories de renseignements qui n'existaient pas lorsque la loi d'habilitation a été adoptée (Brownsword, 2008). Cela peut entraîner une *déconnexion réglementaire*, dans la mesure où la technologie a débordé du cadre juridique correspondant. Il peut être difficile de corriger cette déconnexion et d'adopter des lois qui anticipent l'avenir ou des lois neutres sur le plan technologique (Brownsword, 2008). Par exemple, le fait que la langue soit adaptable à différentes technologies ne signifie pas que l'effet de ces lois sera le même, et il n'est pas toujours possible de faire en sorte qu'une langue adaptable ne procure pas d'avantages (ou n'impose pas de désavantages) à des technologies ou des platesformes données (Reed, 2007). En outre, les lois relatives à la technologie mettent souvent des années à être adoptées et peuvent être en partie caduques à leur entrée en vigueur (Alexander, 2015). De leur côté, les lois adoptées dans la précipitation peuvent avoir des conséquences imprévues (encadré 2.3). En

l'absence d'orientation forte de la part des législateurs ou des tribunaux, les forces de l'ordre peuvent choisir de s'immiscer dans les droits individuels protégés par la Charte de manière inattendue, avec pour conséquence que les tentatives de bonne foi de protéger l'ordre public peuvent s'accompagner de violations mal perçues par la population en général (Parsons et Molnar, 2018).

Encadré 2.3 La SESTA, la FOSTA et le trafic sexuel aux États-Unis

En 2018, les États-Unis ont adopté la loi entravant les activités des trafiquants sexuels (*Stop Enabling Sex Traffickers Act*, ou SESTA) et la loi permettant aux États et aux victimes de lutter contre le trafic sexuel en ligne (*Allow States and Victims to Fight Online Sex Trafficking Act*, ou FOSTA) (Gouv. des États-Unis, 2018). L'intention de ces lois était de freiner le trafic sexuel en criminalisant les platesformes en ligne utilisées pour annoncer des services sexuels (NSWP, 2018). Cependant, à l'instar d'une initiative prise en 1873 par le U.S. Postal Service (le service postal américain) pour éliminer la diffusion de « matériel immoral » (qui a entraîné la saisie de manuels d'anatomie et de matériel de santé génésique en plus de la pornographie), ces lois ont souffert de leur langue générale et ne font pas de distinction entre les travailleurs du sexe victimes du trafic et ceux qui sont consentants (Romano, 2018; Tworek, 2021a).

Si la loi a contraint de nombreux sites Web situés aux États-Unis à surveiller et à supprimer le contenu à caractère sexuel, elle a également créé des dangers pour les travailleurs du sexe consensuels qui recourraient aux platesformes en ligne pour filtrer leurs clients potentiels et partager des renseignements avec d'autres travailleurs du secteur sur des individus potentiellement dangereux ou problématiques (NSWP, 2018; Misitzis, 2021). De nombreux travailleurs du sexe ont dû retourner dans la rue pour attirer les clients (Williams, 2017; Misitzis, 2021). Cela n'a pas surpris de nombreux groupes de défense des travailleurs du sexe, qui ont relevé les conséquences prévisibles d'un langage législatif large (Harmon, 2017). Malheureusement, alors que les conséquences de la SESTA et de la FOSTA sur les travailleurs du sexe consentants sont bien documentées, on ne sait toujours pas si ces lois ont réduit l'incidence du trafic sexuel (Misitzis, 2021).

Le caractère décentralisé d'Internet crée des interdépendances et des difficultés réglementaires en ce qui a trait à la vie privée

Fait peut-être anticipé par la formation précoce d'organismes de renseignement étatiques collaboratifs, tels que le Groupe des cinq (qui réunit l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis)[6], il est désormais évident que les États démocratiques ne peuvent plus définir la confidentialité des données de leurs citoyens de manière isolée; cette définition est nécessairement devenue une question mondiale et s'est étendue pour inclure l'influence des entreprises privées, souvent internationales (Hartzog, 2018; Farrell et Newman, 2019). Bennett et Raab (2018) affirment que cette interdépendance peut aboutir à deux scénarios : (i) les nations qui participent à une « course vers le haut » en cherchant des solutions pour protéger la vie privée des citoyens et (ii) les nations qui participent à une « course vers le bas », dans lesquelles la réglementation est abandonnée en faveur de l'attraction des entreprises.

Dans un autre cadre, Aaronson et Leblond (2018) avancent qu'en raison de la libre et large circulation des données personnelles à travers les frontières, les politiques étatiques peuvent se développer au sein de *domaines* de politiques de données — des États virtuels définis par leurs approches en matière de « politiques fiscales, de transparence, de protection de la propriété intellectuelle, de concurrence et de protection des données, entre autres » [traduction libre]. Les principaux acteurs internationaux qui semblent définir ces domaines sont les États-Unis, l'UE et la Chine (Aaronson et Leblond, 2018), ainsi que le Royaume-Uni.

Malgré la diversité des acteurs, un principe largement accepté, qui figure dans de nombreux cadres de protection de la vie privée et de sécurité, est la *transparence* (Colliver *et al.*, 2021). Tworek et Wanless (2022) affirment toutefois que ce qui constitue exactement la transparence reste à déterminer. Il est donc important que les cadres de transparence proposés soient précis quant aux catégories de renseignements à communiquer et aux personnes qui doivent avoir accès à ces renseignements. Deux concepts proposés comme fondamentaux pour les pratiques concernant la transparence (décrits dans les rapports sur la transparence de la surveillance des entreprises, mais peut-être applicables plus largement) sont les pratiques *vérifiables* et les pratiques *performatives*, les premières étant celles qui diffusent les renseignements appropriés aux bons publics, tandis que les secondes étant celles qui développent et prouvent une culture interne de transparence (il est toutefois également noté que davantage de renseignements ne se traduit pas nécessairement par un meilleur comportement en ligne) (Albu et Flyverbom, 2016; Ballard et Parsons, 2022). Ballard et Parsons (2022) font en outre remarquer que,

6 « Le Groupe des cinq consiste en une alliance des services de renseignements de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Ces pays partenaires échangent un grand éventail de renseignements les uns avec les autres dans le cadre d'une des ententes multilatérales les plus unifiées au monde » (SP, 2021b).

« si ces conceptualisations peuvent être opposées l'une à l'autre, elles pourraient toutes deux être intégrées dans les documents de reddition de comptes sur la transparence, de sorte que ces documents puissent à la fois satisfaire les conditions de vérifiabilité et de performativité » [traduction libre]. Autrement dit, les pratiques de transparence à la fois vérifiables et performatives exigent la diffusion de renseignements utiles, appropriés et pertinents d'une façon constante, dynamique et adaptable.

2.4 Résumé

La vie privée, la sécurité et les droits de la personne font partie intégrante du débat contemporain sur les méfaits en ligne et sur la meilleure façon de les prévenir et de les atténuer. Pour répondre à tous les éléments du mandat, il est essentiel de comprendre la relation entre les méfaits cyberfacilités, la protection de la vie privée et la sécurité des données, ainsi que les moyens particuliers par lesquels les nouvelles technologies numériques sont utilisées pour perpétrer ces méfaits et les possibilités de s'y attaquer.

Comme ce chapitre l'explique, le cadre suivant mérite d'être pris en compte lors de l'évaluation des lois canadiennes sur la protection de la vie privée et la sécurité des données : (i) l'intégration généralisée des TIC dans la vie quotidienne fait que tout le monde est *numérique par défaut* et risque d'être victime de préjudices cyberfacilités; (ii) la vie privée est contextuelle et fondée sur les relations, et les conditions d'utilisation des données recueillies auprès des individus et des communautés reposent sur le consentement et la transparence; (iii) le pouvoir de contrôler l'accès aux données d'un individu ou d'une communauté, ainsi que le recueil et l'utilisation de ces données, est crucial pour garantir la vie privée et la sécurité personnelles et collectives (ou pour y porter atteinte) et (iv) la vie privée et la sécurité des données sont considérées comme des droits de la personne dans certains pays étrangers.

Les TIC sont devenues un élément indispensable de la vie moderne, mais, comme le laisse entendre le mandat, elles ont aussi profondément modifié la manière dont sont commis les actes criminels graves et facilitent toute une série de méfaits en ligne. Leur utilité, leur adoption généralisée et leur potentiel à causer des préjudices ont contraint les organes de réglementation, les décideurs, les chercheurs et le public à adopter une vision de plus en plus nuancée de ce que l'on entend par sécurité et *vie privée*, et de la manière dont la sécurité et la protection de la vie privée jouent un rôle dans l'atténuation ou la prévention des méfaits cyberfacilités. La capacité de créer, de diffuser ou de stocker de grandes quantités d'informations sur Internet peut améliorer la fonctionnalité de nombreux

services, tout en suscitant une foule de problèmes de confidentialité et de sécurité à propos de la protection des renseignements personnels.

Les chapitres suivants examinent les conflits entre la protection de la vie privée, la sécurité et les différents aspects des méfaits cyberfacilités. Le comité d'experts y décrit comment ces méfaits sont favorisés par les technologies numériques, tout en précisant que ces actes se situent sur un spectre d'illégalité, qu'ils visent souvent des groupes démographiques spécifiques et que la criminalisation n'est pas toujours le meilleur moyen de les combattre (chapitre 3). Il examine ensuite certaines des technologies numériques qui permettent ces méfaits, en insistant sur le fait que, bien que ces technologies soient généralement légales, leur nature décentralisée, distribuée et souvent anonyme crée des obstacles importants à la réglementation et à son application lorsqu'elles sont utilisées pour des actes préjudiciables (chapitre 4). Il est possible de s'attaquer à ces méfaits au moyen d'outils et de mesures réglementaires (chapitre 5) ou d'application de la loi (chapitre 6), bien que chacun d'eux se heurte à des défis qui leur sont propres et qui résultent de l'environnement numérique contemporain dans lequel vivent les Canadiens.

3

Technologies numériques et méfaits

Constatations du chapitre

- Les méfaits en ligne se situent sur un spectre de légalité et de criminalité, qui s'étend des infractions criminelles, pour lesquelles il peut être très difficile d'engager des poursuites, aux méfaits préjudiciables, mais légaux.
- Les TIC portent atteinte à la sécurité publique lorsque des individus les utilisent pour faciliter des actes nuisibles. Elles peuvent être employées pour répandre du contenu préjudiciable dans des environnements numériques dont les politiques de modération sont inégales ou inefficaces.
- Tout le monde ne court pas le même risque d'être victime de méfaits en ligne. Les femmes et les jeunes, ainsi que les communautés racisées et minorisées, sont les cibles les plus fréquentes d'actes et de contenu préjudiciables sur Internet.
- La criminalisation n'est pas toujours le moyen le plus efficace de lutter contre les méfaits en ligne ni la méthode d'atténuation privilégiée par les victimes et les survivants.

Si les technologies de l'information et des communications (TIC) présentent de multiples avantages pour la société, elles peuvent également offrir aux individus de nouveaux moyens et voies pour adopter des comportements préjudiciables, ce qui complique les efforts de prévention, de confinement et d'enquête. Dans le même temps, les TIC ont modifié la conception de la vie privée (chapitre 2) et de la manière dont celle-ci est favorisée ou entravée par des mesures visant à garantir la sécurité. Dans ce chapitre, le comité d'experts passe en revue un éventail d'activités préjudiciables dans le but de souligner le fait que leurs conséquences sont plus graves sur certaines personnes et communautés, ainsi que l'importance d'une approche multidimensionnelle et contextualisée pour contrer les méfaits en ligne. Cette approche fait appel à des moyens juridiques et non juridiques, ainsi qu'à l'expérience des victimes et des survivants, lorsqu'il s'agit de choisir les mesures de prévention, d'atténuation et d'indemnisation appropriées.

Le chapitre commence par démontrer comment les progrès des TIC peuvent être utilisés pour faciliter l'exploitation, le harcèlement et la maltraitance de gens, en particulier des femmes, des enfants et des membres de la communauté LGBTIQ+. Certains actes, tels que la diffusion de matériel d'abus pédosexuels (MAP) et de contenu intime non consensuel, constituent des infractions criminelles. Certains

cas de harcèlement en ligne peuvent également faire l'objet de poursuites criminelles, tandis que d'autres ne sont pas considérés comme des comportements criminels ou même illégaux. Quel que soit leur statut juridique, de nombreux cas de harcèlement en ligne causent un préjudice psychologique et ont un effet paralysant sur les victimes. Dans l'ensemble, il demeure difficile de fournir divers types de soutien et d'aide juridique aux victimes et aux survivants de différentes formes de cyberabus criminels et non criminels en raison du manque de ressources et d'informations pour les personnes ciblées, des lacunes réglementaires et des difficultés d'application.

Le chapitre examine ensuite comment les TIC facilitent la diffusion de contenu raciste, xénophobe ou incitant à la violence, au terrorisme et à la propagande haineuse. Bien que la haine et le harcèlement cyberfacilités aient des effets psychologiques dévastateurs et puissent mettre les gens en danger hors ligne, il peut être difficile, dans certains cas, de déterminer avec précision quand le contenu haineux devient illégal et, par conséquent, peut faire l'objet d'une enquête, de poursuites et de sanctions de la part des forces de l'ordre.

Enfin, le chapitre décrit les pratiques frauduleuses facilitées par les TIC, telles que l'extorsion, l'usurpation d'identité et l'accès illégal aux renseignements personnels. Bien que la cyberfraude soit le cybercrime le plus signalé, sa véritable ampleur n'est pas claire en raison des obstacles au signalement. Parmi les différents groupes démographiques, les personnes âgées, les nouveaux immigrants et les jeunes sont particulièrement vulnérables à divers types de pratiques frauduleuses, qui causent des pertes financières importantes et des dommages psychologiques.

Le comité d'experts estime que, si des réformes juridiques peuvent s'avérer nécessaires dans certains cas (p. ex. pour limiter la diffusion d'hypertrucages, abordés à la section 3.1.1), un ensemble d'autres outils de prévention et d'atténuation employés sous l'impulsion de différents acteurs permet également de lutter contre les actes préjudiciables. Les politiques de modération du contenu et les directives communautaires destinées aux fournisseurs de services et aux platesformes de médias sociaux, les tactiques de prévention de la fraude dans les grandes banques et les programmes éducatifs sur les questions liées à la cyberintimidation jouent tous un rôle important dans la réduction de la haine, de la fraude et des abus en ligne. Toutefois, aucune des approches actuelles ne s'attaque pleinement au problème des méfaits cyberfacilités. L'amélioration de la sécurité publique numérique est une cible mouvante, qui nécessite des façons de faire souples fondées sur les difficultés rencontrées par les personnes vivant au Canada.

3.1 Technologies numériques et exploitation, harcèlement et abus

Le Compendium nord-américain sur la classification de la cybercriminalité (NACCC) (section 1.3.2) comprend une catégorie regroupant « l'exploitation, le harcèlement ou l'abus d'une personne » (NACCC, 2021a). Cette catégorie couvre des activités qui sont sans équivoque illégales, comme l'exploitation en ligne des femmes et des enfants (p. ex. la traite des personnes, le MAP, la diffusion de contenu intime non consensuel), ainsi que des activités qui sont illégales quand elles répondent à certains critères, notamment de harcèlement et d'abus en ligne (p. ex. la cyberintimidation). Si tous les types de harcèlement et d'abus sont préjudiciables, la criminalisation n'est pas toujours le moyen le plus efficace de les combattre. Dans les sections suivantes, le comité d'experts décrit la légalité de ces actes, dans la mesure du possible, afin d'éclairer les pratiques nouvelles ou prometteuses.

3.1.1 Exploitation en ligne des femmes et des enfants

Les femmes et les jeunes sont surreprésentés parmi les cibles de la violence en ligne (Henry et Powell, 2016; Bailey *et al.*, 2017). L'exploitation des femmes et des enfants en ligne comprend des activités allant de la traite des personnes à la publication de contenu intime non consensuel. Si les TIC ont changé la façon dont les femmes et les enfants sont exploités, la violence en ligne se trouve sur un continuum fondé sur le genre et l'âge dans la société en général (ASPC, 2019; Khoo, 2021).

Les TIC facilitent la traite des femmes et des enfants

Effectuer la traite des personnes est défini comme le fait « de recruter, de transporter et de loger des personnes ou d'exercer un contrôle ou une influence sur leurs mouvements afin de les exploiter, généralement à des fins sexuelles ou de travail forcé » (JUS, 2021). La traite des femmes et des enfants est l'entreprise criminelle qui connaît la croissance la plus rapide au monde, elle enregistre un profit annuel estimé à 99 milliards de dollars US (Equality Now, 2019). Au Canada et ailleurs, les trafiquants utilisent Internet pour publier des annonces, faire le commerce de femmes et d'enfants sur des sites Web et entrer en contact avec les acheteurs et participer à des clavardoirs et autres forums Internet pour entrer en contact avec des victimes potentielles (Equality Now, 2019; Baird *et al.*, 2020). Les marchés en ligne de location de logements temporaires (p. ex. Airbnb) peuvent également faciliter la traite des personnes, car ils permettent un plus grand anonymat des locataires, ce qui rend plus difficile pour la police de recueillir des renseignements utiles. Ils sont également soumis à une réglementation et à des mécanismes d'application de la loi moindres que les établissements licenciés, comme les hôtels (Mcquigge, 2018; O'Regan, 2019; Binns et Kempf, 2021).

Les femmes et les filles représentent 95 % des victimes du trafic sexuel au Canada et elles sont âgées de 18 à 24 ans dans 43 % des cas (Ibrahim, 2021). Outre le sexe et l'âge, les autres facteurs de risque communs aux victimes de la traite sont le statut d'immigrant, le fait d'être passé par le système de protection de l'enfance, l'instabilité financière ou sociale et l'appartenance autochtone (SP, 2021c). Les femmes autochtones sont régulièrement surreprésentées dans le commerce du sexe au Canada (AFAC, 2014), et des études montrent que leur recrutement est de plus en plus facilité par les médias sociaux, notamment par des platesformes courantes comme Facebook (Louie, 2017). Lors d'entretiens qu'il a menés en Alberta, Louie (2017) a constaté que Facebook était un des principaux outils utilisés pour recruter des adolescents et des jeunes femmes dans les réserves des Premières Nations environnantes et les attirer dans les villes à des fins d'exploitation sexuelle. Après le recrutement, Facebook et d'autres applications de médias sociaux étaient utilisés pour organiser de prétendus « rendez-vous » et permettaient aux victimes de la traite de rester en communication constante avec leurs exploiteurs. Ces actions nuisaient à la sécurité des espaces ouverts pour les jeunes à risque, notamment les centres communautaires et culturels et les programmes parascolaires dans les réserves.

À cause du recours à des outils de médias sociaux qui dissimulent les tentatives de recrutement aux parents et aux éducateurs, il est de plus en plus difficile de cerner les filles et les femmes autochtones à risque (Louie, 2017). En outre, le déplacement des réseaux de traite des personnes de la rue vers Internet a fait en sorte que les victimes sont moins visibles et plus difficiles à détecter et à aider pour les travailleurs de proximité ou les policiers. Dans la lutte contre l'exploitation sexuelle des filles et des femmes dans les communautés des Premières Nations, Louie (2017) souligne l'importance d'effectuer des interventions précoces et globales qui tiennent compte des besoins de la communauté et de la culture.

Internet permet une large diffusion du MAP

Les TIC ont rendu possible le partage illégal du MAP plus facilement que ce n'était le cas autrefois (Negreiro, 2020). Les délinquants pédosexuels tirent profit des technologies numériques pour communiquer avec d'autres délinquants du monde entier, ainsi que pour partager des images et des renseignements sur la façon de leurrer les enfants ou de dissimuler leur empreinte numérique (Negreiro, 2020). Ils trouvent souvent un soutien et une légitimation de leurs activités et de leur comportement dans les communautés en ligne (Jeney, 2015). Ils utilisent également les TIC pour communiquer avec des victimes potentielles et les manipuler, utilisant souvent ces outils pour attirer les mineurs afin de les rencontrer en personne ou de les contraindre à effectuer des actes sexuellement explicites en ligne (UNODC, 2015; Negreiro, 2020).

Bien qu'il n'existe pas de calcul exact du volume de MAP en ligne (Edwards *et al.*, 2021), de nombreuses données probantes indiquent que la diffusion et la circulation des TIC ont eu des effets correspondants sur la création et la circulation de MAP et sur l'exploitation des enfants en général. L'Internet Watch Foundation (IWF) a constaté une augmentation de 16 % entre 2019 et 2020 du nombre de signalements confirmés de MAP sur Internet (IWF, 2020) et le Centre canadien de protection de l'enfance (CCPE) a fait état d'une hausse constante de la détection de MAP à supprimer entre 2018 et 2020 (CCPE, 2021). Ces augmentations peuvent être liées, en partie, à la pandémie de COVID-19, durant laquelle les délinquants sexuels et les enfants ont passé plus de temps en ligne (Negreiro, 2020; UN News, 2020; NCMEC, 2021). Si le Web clandestin (*Dark Web*) (chapitre 4) a joué un rôle important en orientant les délinquants sexuels pédophiles vers des sites hébergeant du MAP, la majorité des images trouvées par le programme de détection du MAP Projet Arachnid (encadré 6.1) étaient hébergées sur le Web ouvert, sur des platesformes telles que Twitter, Facebook, des applications de messagerie ou des sites Web de stockage d'images et de fichiers (Kristof, 2020; CCPE, 2021).

Les filles sont plus susceptibles d'être victimes de l'exploitation en ligne de mineurs. Un rapport du CCPE a démontré que 80 % des dizaines de milliers d'images uniques d'exploitation ou d'abus sexuels évaluées représentaient des filles (CCPE, 2016). De plus, 78 % de ces images représentaient des enfants de moins de 12 ans, près de 50 % d'entre eux semblant avoir moins de 8 ans. Le CCPE avance que ces chiffres ne traduisent pas l'étendue réelle probable des abus commis à l'encontre des mineurs postpubères, parce que la technologie et la base de données utilisées pour déceler les abus sont biaisées en faveur des victimes jeunes et parce que les victimes plus âgées sont moins susceptibles de demander de l'aide en raison de la peur, de la honte ou de la possibilité de voir les images de leurs abus visionnées à répétition (CCPE, 2021).

La suppression de MAP se heurte à des écueils, notamment parce que certains fournisseurs de services ne prennent pas les mesures de modération du contenu permettant de bloquer les images illégales lorsqu'elles sont téléversées par les utilisateurs (CCPE, 2021). Dans de nombreux cas, ils s'opposent également à des demandes spécifiques de suppression de MAP parce que les modérateurs de contenu supposent que ce matériel représente un adulte. Cela retarde la suppression du contenu illégal et permet sa propagation (CCPE, 2021). Certaines entreprises privées ont établi des politiques qui limitent l'accès et la diffusion de MAP. Par exemple, en 2020, Visa, Mastercard et Discover ont mis fin à l'utilisation de leurs cartes sur le site Web Pornhub, basé au Canada, après que des enquêtes ont confirmé que de nombreuses vidéos qui y étaient publiées mettaient en scène l'agression sexuelle d'enfants (Goodwin, 2020; Kristof, 2020; Price, 2022). Pornhub

a alors interdit aux téléverseurs non vérifiés de publier du nouveau contenu et a supprimé au moins 10 millions de vidéos publiées par ces derniers (Kan, 2020). En tant que telle, cette intervention privée a amené des changements importants dans la politique de modération du contenu de Pornhub (Pornhub, 2020).

La diffusion de contenu intime non consensuel peut provoquer la honte, l'anxiété, la dégradation de la santé physique et la détérioration des relations

Les gens peuvent volontairement produire et partager des images intimes d'eux-mêmes. Cependant, ces images intimes peuvent également être diffusées ultérieurement sur des sites Web ou des médias sociaux sans consentement (Daswani et Pearson, 2014; Short *et al.*, 2017; Bothamley et Tully, 2018). Dans certains cas, les images diffusées sont captées à l'insu de la personne par piratage ou par le biais de vidéos de surveillance (Citron et Franks, 2014; Henry et Powell, 2016; Short *et al.*, 2017). Ces actes sont parfois qualifiés de *vengeance pornographique*, bien que ce terme soit impropre, car les raisons de la distribution peuvent aller au-delà de la vengeance et inclure le chantage, l'intimidation et le plaisir (Henry et Powell, 2016). En outre, ce terme pourrait minimiser le préjudice causé aux victimes, car la pornographie est notoirement difficile à définir et peut dépendre du point de vue de la personne qui regarde l'image (Henry et Powell, 2016).

Si tout le monde peut être victime de la diffusion de contenu intime non consensuel, ce crime est plus susceptible d'affecter les femmes et les filles (Henry et Powell, 2016; Short *et al.*, 2017). Les victimes font souvent état d'une forte anxiété, de honte, d'effets nuisibles sur leur santé physique, ainsi que de dommages à leur carrière et à leurs relations (Short *et al.*, 2017; Wells, 2019) (récit 2). Il existe des milliers de sites Web consacrés à la diffusion de contenu intime non consensuel — on estime qu'il y en avait 2 000 en 2017 (Short *et al.*, 2017) — ainsi qu'un certain nombre d'autres qui, sans avoir été spécialement créés pour cela, peuvent être assimilés à cette fin (p. ex. Pornhub). Beaucoup de ces sites peuvent porter ombrage à long terme aux victimes et aux survivants, car les empreintes numériques peuvent rester en ligne longtemps et être téléchargées et partagées par plusieurs utilisateurs et sur plusieurs platesformes (Dodge, 2019).

Récit 2 L'origine de Women Against Cyberrape

En 2010, Rebekah Wells était en train de chercher son nom sur Google lorsqu'elle a découvert une galerie en ligne de photos d'elle-même, nue. Les photos explicites, ainsi que ses coordonnées, avaient été publiées par un ex-petit ami à son insu et sans son consentement, deux ans après la fin de leur relation. Elles sont apparues sur plusieurs sites pornographiques commerciaux, où les utilisateurs ont laissé des commentaires misogynes en dessous. Certains utilisateurs malveillants ont indiqué à madame Wells qu'ils avaient téléchargé les images et lui ont rappelé que ses photos où elle est nue ne pourraient jamais être totalement supprimées d'Internet.

M^{me} Wells a porté plainte à son poste de police et a finalement pu intenter une action en justice contre son ex-petit ami, le site d'hébergement et Cloudflare, le serveur mandataire prenant en charge le site d'hébergement. Si les images ont été retirées de ce dernier site, elles ont continué à apparaître sur d'autres sites pornographiques. M^{me} Wells a subi un stress émotionnel, psychologique et physique. Elle a été hospitalisée pendant un an après avoir perdu plus de 20 livres. En novembre 2012, elle a fondé l'organisme Women Against Cyberrape (anciennement Women Against Revenge Porn) afin de soutenir et de guider les autres victimes de ce genre de méfait. Son expérience l'a également incitée à s'inscrire dans une école de droit en 2017, et elle est aujourd'hui avocate pour les droits des victimes en Floride.

(Wells, 2019, s.d.-a,-b)

Il demeure difficile de détecter la diffusion de contenu intime non consensuel, de légiférer sur le sujet et d'engager des poursuites

La législation relative à la diffusion de contenu intime non consensuel évolue. Au Canada, en vertu de l'article 162.1 du *Code criminel*, la diffusion non consensuelle d'images intimes, quel que soit l'âge des personnes concernées, est illégale (GC, 1985; Dodge et Spencer, 2018) et plusieurs provinces et territoires disposent de lois civiles concernant le contenu intime non consensuel (Laidlaw et Young, 2020). Depuis la promulgation de ces dernières, le nombre de cas signalés dans chaque province et territoire a augmenté (Allen, 2019). Toutefois, en 2021, seulement 17 % de ces signalements à la police au Canada ont donné lieu à des accusations (StatCan, 2022).

Afin de mieux harmoniser les lois dans tout le Canada, Laidlaw et Young (2020) recommandent l'adoption de textes législatifs qui accéléreraient les procédures visant à forcer un défendeur ou (plus probablement) un tiers intermédiaire (p. ex. Google) à retirer le contenu illicite et à désindexer les résultats de recherche, ainsi que de lois civiles qui permettraient aux plaignants d'obtenir des dommages-intérêts si des preuves claires de préjudice sont fournies. Cependant, comme il est indiqué ailleurs dans ce rapport, même si une affaire fait l'objet de poursuites au Canada, les images peuvent exister hors de la juridiction canadienne. La loi peut avoir un pouvoir limité sur les pays qui hébergent les sites et sur les étrangers situés ailleurs dans le monde qui distribuent les images (Henry et Powell, 2016).

Afin de compléter les voies légales, certains sites, comme OnlyFans, ont mis en place des contrôles supplémentaires pour les créateurs de contenu, afin de s'assurer que la plateforme ne propose pas de services à des mineurs ou à des personnes utilisant une fausse identité, ou ne recueille pas de données personnelles auprès d'eux. Ces contrôles consistent à exiger une copie de passeport et un égoportrait des créateurs tenant leur carte d'identité officielle et à recourir à un logiciel d'analyse faciale pour vérifier leur identité (OnlyFans, 2020). Pornhub a aussi mis en place des politiques et des mécanismes d'application et de modération (notamment des outils numériques) pour signaler et supprimer le contenu non consensuel (Pornhub, 2022), mais de nombreux sites — notamment ceux consacrés au contenu non consensuel — ne l'ont pas imité (Dodge, 2019).

La technologie d'hypertrucage est utilisée pour créer des images et des vidéos intimes non consensuelles

Les procédés *d'hypertrucage* (encadré 3.1) présentent un intérêt dans certains contextes pour la production de films et de jeux, et ont également des applications pour les soins de santé. En dehors du mérite artistique ou satirique additionnel que cette technologie peut avoir, la facilité avec laquelle elle peut être utilisée pour nuire a fait de sa détection une priorité des organismes gouvernementaux (Chesney et Citron, 2019; Rao *et al.*, 2021). Les premières craintes à propos de l'usage de l'hypertrucage ont porté sur les risques qu'il présente pour la démocratie, la stabilité politique, les célébrités et les politiciens (Ajder *et al.*, 2019; Chesney et Citron, 2019). Cependant, un rapport publié par DeepTrace — un chef de file de l'industrie en matière de renseignement sur les menaces visuelles — a conclu que cette technologie est en grande partie utilisée pour créer des images intimes non consensuelles (Ajder *et al.*, 2019). De plus, il a été constaté que les femmes constituaient les cibles exclusives sur les cinq sites Web de fausse pornographie les plus populaires (Ajder *et al.*, 2019).

Encadré 3.1 L'hypertrucage

L'hypertrucage est une forme de média synthétique qui applique des techniques d'apprentissage machine pour « fusionner, combiner, remplacer et superposer des images et des clips vidéo » [traduction libre] afin de créer des vidéos ou des images apparemment authentiques de quelqu'un ou de quelque chose qui n'est pas réel (Maras et Alexandrou, 2018). Des logiciels (p. ex. Adobe After Effects) et des programmes en source ouverte (p. ex. Face Swap, DeepFaceLab ou FakeApp) permettent de produire du contenu audio et vidéo réaliste, à condition que le créateur dispose de suffisamment de données de référence, comme des images fixes, des clips vidéo et des échantillons de voix (Maras et Alexandrou, 2018; Paris et Donovan, 2019).

Le montage par hypertrucage se distingue des techniques traditionnelles de montage médiatique et d'imagerie générée par ordinateur par son recours à des algorithmes d'apprentissage profond (Khoo *et al.*, 2021). Ces algorithmes *entraînent* le système à reproduire les caractéristiques d'une personne sur une autre — généralement en montrant au programme de nombreuses heures de vidéo d'une personne filmée sous différents angles et sous différents éclairages (Adee, 2020). L'entraînement s'effectuant souvent de manière autonome, il est possible pour les développeurs de créer des programmes dont le fonctionnement ne nécessite que peu ou pas d'expertise technique (Khoo *et al.*, 2021). Dans de nombreux cas, ces programmes sont offerts gratuitement sur des dépôts de logiciels ouverts tels que GitHub, tandis que les utilisateurs de forums comme Reddit peuvent être là pour aider au dépannage (Tolosana *et al.*, 2020; Khoo *et al.*, 2021). Certains hypertrucages peuvent être difficiles à repérer, même à l'aide d'un logiciel spécial. La difficulté de détecter les manipulations dépend, entre autres, « du degré de compression, de la résolution de l'image et de la composition de l'ensemble de test » [traduction libre] (Bernaciak et Ross, 2022).

La plupart des hypertrucages pornographiques utilisent des techniques recourant à des supports réels, qu'ils modifient pour représenter des informations « non contenues dans les données originales ou non conformes à la réalité » [traduction libre] (Khoo *et al.*, 2021). La manipulation d'images peut prendre plusieurs formes et servir à travestir l'identité d'une personne représentée sur le support (p. ex. par permutation de visages), à travestir les attributs ou les caractéristiques d'une personne (p. ex. sa couleur de peau ou les traits de son visage) ou à modifier les expressions faciales, les mouvements du visage ou les paroles d'une personne — en fait, à mettre dans sa bouche des mots qu'elle n'a jamais prononcés (Tolosana *et al.*, 2020).

Grâce à ces techniques, un individu peut incorporer de manière réaliste le visage et la voix d'une victime dans des vidéos compromettantes (Cook, 2019) et simuler le retrait de ses vêtements avec une simple image ou vidéo du sujet (fait notable, la plupart des programmes s'appuyant sur des applis pour générer du contenu intime non consensuel ne fonctionnent que sur des corps représentant des femmes) (Cook, 2021). Les images et les vidéos de célébrités étant largement accessibles, la fausse pornographie cible principalement les femmes célèbres. Cependant, il existe également des comptes rendus de femmes et d'enfants non célèbres ayant subi des attaques similaires, souvent dans le cadre d'un chantage ou de la diffusion de contenu intime non consensuel, ou pour humilier ou traumatiser la victime d'une autre manière (MacDonald, 2021). Les femmes dont le corps figure dans ces vidéos sont également des victimes parce que leur représentation est utilisée à leur insu et sans leur consentement (Paris et Donovan, 2019; MacDonald, 2021).

Il y a un vide réglementaire dans la lutte contre le contenu hypertruqué

Les outils réglementaires et juridiques actuels, au Canada comme ailleurs, sont fragmentés et mal conçus pour lutter contre les méfaits associés à l'hypertrucage (Chesney et Citron, 2019; Karasavva et Noorbhai, 2021). Certains de ces méfaits peuvent constituer des crimes s'ils comprennent du MAP en ligne (Karasavva et Noorbhai, 2021) et le *Code criminel* canadien sanctionne la distribution d'images intimes (notamment au moyen de films ou d'enregistrements vidéo) sans le consentement du sujet (GC, 2014). Toutefois, la question de savoir si les hypertrucages synthétisés par des algorithmes relèvent de cette définition est sujette à interprétation (Karasavva et Noorbhai, 2021). Au-delà des accusations criminelles, il est possible d'appliquer les lois sur le droit d'auteur et sur la diffamation aux cas d'hypertrucage, chacune ayant des limites particulières (Chesney et Citron, 2019; Karasavva et Noorbhai, 2021).

Une interdiction complète de l'hypertrucage pourrait avoir des conséquences négatives involontaires étant donné les utilisations bénéfiques de la technologie (p. ex. dans la réalisation de films), tout en portant atteinte à la liberté de parole et d'expression (Chesney et Citron, 2019; Karasavva et Noorbhai, 2021). Karasavva et Noorbhai (2021) ont avancé qu'il serait plus approprié d'étendre les lois canadiennes existantes pour y inclure un langage plus spécifique aux images et aux vidéos intimes faussement créées. Chesney et Citron (2019) suggèrent de faire en sorte qu'il soit plus facile pour les citoyens privés de poursuivre les platesformes pour la diffusion de contenu nuisible téléchargé par leurs utilisateurs, afin de les inciter à supprimer rapidement le contenu hypertruqué. Cette approche peut toutefois conduire au retrait excessif de contenu légal (chapitre 5).

3.1.2 Harcèlement et abus en ligne

Le harcèlement et les abus en ligne prennent de nombreuses formes et peuvent viser un collectif (p. ex. par la formulation de commentaires haineux à grande échelle), des individus (p. ex. par le cybertraquage) ou les deux (p. ex. par la cyberintimidation). Le harcèlement et les abus peuvent être liés aux relations personnelles (p. ex. le divorce) ou à des identités sociales et culturelles larges (p. ex. la race, le sexe, la religion). Comme l'illustre cette section, de nombreux cas d'exacerbation et de nuisance préjudiciable en ligne ne sont pas considérés comme des comportements criminels. Le comité d'experts utilise le terme de *harcèlement* au sens large pour englober à la fois les infractions criminelles et les actes préjudiciables non criminels. Déterminer si un acte constitue une infraction criminelle est un défi, et la criminalisation n'est pas nécessairement la voie la plus efficace ou préférable pour traiter tous les méfaits en ligne.

Le cyberharcèlement et les abus en ligne sont considérés comme des crimes dans certains cas

Selon le *Code criminel* canadien, le harcèlement criminel désigne un comportement répété qui amène une personne à « lui faire raisonnablement craindre — compte tenu du contexte — pour sa sécurité ou celle d'une de ses connaissances » (GC, 1985). La cyberintimidation consiste à utiliser les TIC pour « intimider ou harceler une autre personne » (GRC, 2021c). Certaines formes de cyberharcèlement, de cybertraquage et de cyberintimidation peuvent faire l'objet d'une enquête et de poursuites en vertu de l'article 264 du *Code criminel* si elles sont considérées comme du harcèlement criminel ou si elles comprennent la profération de menaces (GC, 1985). Les logiciels traqueurs sont utilisés pour harceler ou intimider les victimes ou pour surveiller secrètement leurs messages ou leur activité en ligne (Khoo *et al.*, 2019). Ces logiciels sont largement accessibles aux consommateurs et peuvent « permettre un accès en temps réel et à distance aux messages texte, aux courriels, aux photos, aux vidéos, aux appels téléphoniques entrants et sortants, à la localisation GPS, aux mots de passe de comptes bancaires ou autres, aux comptes de médias sociaux, et plus encore » [traduction libre] (Khoo *et al.*, 2019), ce qui peut constituer des infractions criminelles en vertu du droit canadien (GC, 1985).

Bien que le cyberharcèlement, le cybertraquage et la cyberintimidation se produisent en ligne, soit publiquement (p. ex. par le biais des médias sociaux ou d'articles de blogue) ou sur des canaux privés (p. ex. par courriel ou messagerie directe), ils sortent souvent du cadre numérique pour se traduire par du traquage et des contacts physiques (Al-Khateeb *et al.*, 2017; Brown *et al.*, 2017). Il est de plus en plus fréquent, en effet, que les outils numériques soient utilisés pour perpétrer

des crimes hors ligne liés au traquage ou au harcèlement. Par exemple, des logiciels espions facilement accessibles peuvent surveiller les mouvements physiques d'une victime (Khoo *et al.*, 2019).

Les jeunes, les femmes et la communauté LGBTIQ+ sont des cibles courantes du harcèlement en ligne

Une enquête mondiale menée auprès de 14 000 filles et jeunes femmes âgées de 15 à 25 ans, dans 22 pays, a révélé que 58 % d'entre elles ont été victimes d'une forme de harcèlement en ligne (Plan International, 2020a). Les formes les plus courantes de harcèlement sont les propos injurieux ou insultants (59 %), le discrédit (41 %), le dénigrement de l'apparence (39 %) et les menaces de violence sexuelle (39 %). En outre, 37 % des filles qui s'identifient comme appartenant à une minorité ethnique ont été harcelées en raison de cette particularité, tandis que 56 % des personnes qui s'identifient comme LGBTIQ+ ont déclaré des abus spécifiquement liés à cette partie de leur identité. Dans l'ensemble, cependant, les recherches sur la relation entre l'attaque cybernétique et l'identité LGBTIQ+ sont limitées (Abreu et Kenny, 2018). Les abus en ligne se sont produits sur toutes les grandes platesformes, mais c'est sur Facebook (39 %) que les personnes interrogées en ont signalé le plus (Plan International, 2020a).

Les femmes sont également ciblées de manière disproportionnée par le recours aux logiciels espions et aux logiciels malveillants, et ces outils sont souvent employés dans le cadre de violence, de harcèlement et d'abus conjugaux (Shahani, 2014; Siminovic, 2017; Khoo *et al.*, 2019). De plus, le chevauchement entre traquage physique et cybertraquage est particulièrement prononcé chez les femmes; pour beaucoup, le cybertraquage est une facette ou une extension de la violence domestique qu'elles subissent dans le monde réel (Nobles *et al.*, 2014; Henry et Powell, 2016; Al-Khateeb *et al.*, 2017).

Il est prouvé que les jeunes, les femmes et les membres de la communauté LGBTIQ+ au Canada sont particulièrement vulnérables à la cyberintimidation et au harcèlement en ligne, et que ces actes peuvent entraîner des préjudices psychologiques et physiques importants (Hango, 2016; Broll *et al.*, 2018; Lam *et al.*, 2019). Par exemple, 17 % des jeunes Canadiens (15 à 29 ans) qui ont utilisé Internet entre 2009 et 2014 ont été victimes de cyberintimidation ou de cybertraquage (Hango, 2016). Il s'agit généralement d'attaques soutenues plutôt que d'événements ponctuels. Une enquête auprès des jeunes a révélé que, pour 65 % de ceux qui avaient été victimes de cyberintimidation au cours du dernier mois, celle-ci avait commencé plus d'un an auparavant (PrevNet, 2014).

L'appartenance autochtone est un facteur de risque de harcèlement en ligne

Les publications sur le cyberharcèlement montrent que l'appartenance autochtone augmente le risque de certaines formes d'attaque cybernétique. Des études révèlent que l'utilisation accrue des médias sociaux a fait des jeunes et des femmes autochtones des cibles plus faciles pour la haine, le racisme et l'intimidation en ligne (Bailey et Shayan, 2016; Rice *et al.*, 2016), ce qui souligne la nature intersectionnelle du harcèlement en ligne. Dans une étude portant sur 204 jeunes Autochtones (âgés de 10 à 16 ans) vivant dans une réserve du Conseil tribal de Saskatoon, 30 % des élèves ont déclaré avoir été victimes de cyberintimidation au cours du mois précédent (Lemstra *et al.*, 2011). En comparaison, 10 % des élèves de la même tranche d'âge ont déclaré avoir été victimes de cyberintimidation dans la ville de Saskatoon.

Bien que les données de cette étude — et dans ce domaine de recherche dans son ensemble — soient limitées, elles indiquent que les jeunes Autochtones vivant en réserve sont victimes de cyberintimidation (et d'autres formes d'intimidation) dans une proportion supérieure à la moyenne nationale (Lemstra *et al.*, 2011).
Les données limitées et la relation entre l'appartenance autochtone et les préjudices en ligne montrent qu'il est nécessaire que les chercheurs et les responsables politiques accordent davantage d'attention à cette question. En outre, il est « nécessaire d'effectuer des recherches qui traitent l'appartenance autochtone comme plus qu'une simple variable ou comme une entité monolithique ou une identité statique » [traduction libre] (Huey et Ferguson, 2022). Cette recherche « se penchera sur les diverses intersections entre l'appartenance autochtone, d'une part, et la classe, le genre, le sexe et d'autres facteurs, d'autre part, pour créer des canaux de risque uniques » [traduction libre] (Huey et Ferguson, 2022).

Certaines professions sont souvent la cible de harcèlement en ligne

Certaines professions exigeant une présence sur Internet sont plus susceptibles d'être la cible de harcèlement en ligne. Par exemple, une enquête a révélé que 65 % des journalistes au Canada — en majorité des femmes — ont reçu des menaces ou ont été harcelés en ligne au moins une fois au cours des 12 mois précédents et que 20 % d'entre eux en ont fait l'expérience quotidiennement ou hebdomadairement (Ipsos, 2021). De plus, les attaques sur Internet contre les femmes journalistes semblent augmenter, tant à l'échelle mondiale qu'au Canada (Ipsos, 2021; Posetti *et al.*, 2022). Les images ou messages à caractère sexuel et les menaces physiques sont les formes les plus courantes de harcèlement en ligne dont sont victimes les journalistes, ce qui conduit près d'un tiers des personnes interrogées à envisager de quitter la profession (Ipsos, 2021). Outre les journalistes, les chercheurs,

les communicateurs en santé publique et les politiciens — en particulier les femmes — sont également très susceptibles d'être harcelés en ligne (Tenove et Tworek, 2020; Wagner, 2022; Wright *et al.*, 2022).

Le harcèlement et les abus en ligne causent des dommages psychologiques et limitent la liberté d'expression

Le harcèlement et les abus en ligne sont vécus à l'échelon individuel et sociétal. Si les conséquences varient selon le genre de préjudice, les cibles du harcèlement en ligne courent un risque accru d'anxiété et de dépression. Même lorsqu'il n'y a pas de contact physique, les victimes de cybertraquage peuvent souffrir de graves effets sur leur santé mentale, qui nuisent à leurs relations et à leur carrière et peuvent conduire, entre autres, à l'isolement (Strawhun *et al.*, 2013; Al-Khateeb *et al.*, 2017). Comme pour l'intimidation physique, les jeunes qui subissent de la cyberintimidation ont plus de risques de souffrir de dépression et d'anxiété que leurs pairs non intimidés (Wang *et al.*, 2011; Broll et Huey, 2015; Abreu et Kenny, 2018). Contrairement à ce qui se passe avec l'intimidation physique et verbale dans la cour de récréation, les applications de médias sociaux permettent d'atteindre les cibles bien après les heures de cours et dans l'enceinte de leur propre maison. De ce fait, ils n'ont que peu de répit face à l'intimidation et peuvent avoir plus de mal à échapper à ses impacts (Broll et Huey, 2015).

Le harcèlement et les abus en ligne ont des répercussions négatives qui ne se limitent pas à l'individu. L'enquête mondiale de Plan International a révélé que le harcèlement en ligne peut amener de nombreuses filles et jeunes femmes à quitter les médias sociaux (12 %), à moins les utiliser (19 %) ou à modifier leur façon de s'exprimer en ligne (12 %) (Plan International, 2020b). Le harcèlement en ligne des filles et des femmes a des conséquences sociales, comme l'a fait remarquer la directrice générale de Plan International lors de la publication des résultats de l'enquête de l'organisme : « Ces attaques ne sont peut-être pas physiques, mais elles sont souvent menaçantes, implacables et limitent la liberté d'expression des filles. Exclure les filles des espaces numériques est extrêmement dommageable pour leur autonomie dans un monde de plus en plus numérique, et nuit à leur capacité à être vues et entendues et à devenir des leaders » [traduction libre] (Plan International, 2020a).

Le harcèlement et les abus en ligne ont un effet paralysant

Les menaces et le harcèlement en ligne ont souvent pour but de réduire au silence les voix des victimes — ou de les paralyser —, qui sont de manière disproportionnée des femmes et des membres de groupes marginalisés (Pew Research Center, 2017). Cet effet est dramatique et a conduit des femmes et des filles à autocensurer leurs points de vue et leurs opinions dans les espaces non numériques par crainte

d'abus ou de réaction hostile (Jankowicz *et al.*, 2021). D'autres femmes se sont retirées de la politique ou du militantisme social, ou ont reconsidéré la poursuite d'une carrière dans ces domaines, en raison du potentiel d'abus en ligne (Campbell et Lovenduski, 2016; Di Meco, 2019; Jankowicz *et al.*, 2021). Ces abus peuvent menacer les fondements de la démocratie participative en ciblant des voix et des perspectives diverses, nouvelles ou autres (Citron et Penney, 2019).

Cet effet paralysant a des répercussions dans d'autres domaines d'expertise que la politique et le militantisme, et influe sur la qualité des renseignements communiqués par les experts et mis à la disposition du public. Par exemple, dans une enquête menée par *Nature* auprès de plus de 300 scientifiques qui avaient été interrogés dans les médias sur la pandémie de COVID-19, plus des deux tiers des répondants ont fait état d'expériences négatives consécutives à leur apparition dans les médias ou à leurs déclarations dans les médias sociaux (Nogrady, 2021). Si les attaques contre la crédibilité étaient la forme d'abus en ligne la plus signalée, 22 % des personnes interrogées ont reçu des menaces de violence physique ou sexuelle, tandis que 15 % ont déclaré avoir reçu des menaces de mort.

À l'instar d'autres études sur les abus en ligne, *Nature* a constaté que les femmes, les personnes de couleur et les membres des groupes marginalisés étaient plus souvent la cible d'abus en ligne et que les commentaires désobligeants qu'ils recevaient étaient souvent de nature personnelle (c.-à-d. à propos du sexe, de la race ou de l'origine ethnique), au lieu de viser leurs opinions ou leur érudition. Les menaces en ligne ont eu des effets profonds sur les personnes interrogées. Dans un exemple type d'effet paralysant, les scientifiques qui ont été victimes de trollage ou d'attaques personnelles sur Internet ont indiqué qu'ils étaient désormais moins susceptibles de parler aux médias ou de communiquer leurs résultats et leurs opinions professionnelles au public (Nogrady, 2021). La décision de se retirer du paysage médiatique a des conséquences tangibles sur l'avancement professionnel, en particulier chez les jeunes chercheurs, sur la relève et sur les femmes, qui peuvent perdre de précieuses occasions d'étoffer leur profil professionnel (Nogrady, 2021).

Il est difficile de poursuivre le harcèlement et les abus en ligne

Il peut être difficile de poursuivre des crimes en ligne comme le cybertraquage. Dans certains cas, le langage offensant peut être considéré comme une expression de la liberté d'expression; dans d'autres cas, les victimes peuvent ne pas signaler les abus commis dans des communications privées ou ne pas savoir qu'elles peuvent signaler le contenu préjudiciable aux fournisseurs de services (Al-Khateeb *et al.*, 2017). La plupart du temps, elles n'ont pas accès à des renseignements ou à des ressources sur ce qu'elles doivent faire si elles sont harcelées sur le Web (Ketchum, 2020) et éprouvent un sentiment de honte ou la crainte de représailles;

ce sentiment peut les inciter à ne pas défendre leur cause (Al-Khateeb *et al.*, 2017). Enfin, selon le pays, les victimes peuvent devoir subir une certaine dose de harcèlement ou de traquage avant d'avoir le droit de porter plainte (Al-Khateeb *et al.*, 2017). Malgré les nombreuses preuves documentant les abus et le harcèlement dont des femmes font l'objet en ligne, et certaines mesures prises par les entreprises technologiques, le problème persiste (Khoo, 2021). Il a été avancé que l'inefficacité de la réponse était due, en partie, au secteur technologique lui-même, où la diversité sexuelle et raciale est faible à tous les niveaux, y compris aux postes de direction et de gestion (Khoo, 2021).

La vente de logiciels traqueurs et d'outils de harcèlement facilite le cyberharcèlement (encadré 3.2). Si l'outil technologique est vendu dans le but déclaré d'espionner les communications personnelles d'autrui, par exemple, les développeurs et les vendeurs canadiens pourraient être tenus criminellement responsables. Dans ce cas, les développeurs et les vendeurs pourraient également fait l'objet de poursuites civiles intentées par des victimes et des survivants. Toutefois, il est plus fréquent que ces applications soient mises au point et vendues à des fins tout à fait légales (p. ex. pour surveiller les enfants et les employés), mais réutilisées à des fins malveillantes. Prouver la culpabilité peut alors être difficile (Khoo *et al.*, 2019).

Encadré 3.2 Nouveaux problèmes de sécurité posés par les petits dispositifs de traçage

Comme la commercialisation des nouveaux produits de TIC fait l'objet d'une surveillance réglementaire ou d'une préparation faible, ces produits peuvent causer des préjudices involontaires qui ont des conséquences sur la sécurité et la vie privée. Les AirTag d'Apple et les dispositifs similaires, tels que le Tile, le Galaxy SmartTag de Samsung et le Chipolo ONE, sont des exemples de dispositifs de surveillance légaux pouvant servir à des fins criminelles; ce phénomène pose des problèmes aux forces de l'ordre lorsqu'elles doivent réagir à ces nouvelles techniques criminelles. Les petits dispositifs de suivi sont conçus pour aider les gens à retrouver leurs effets personnels (p. ex. des clés, un sac à main, un sac à dos) au moyen d'une application mobile et du Bluetooth (Apple, 2022; Samsung, s.d.; Tile, s.d.). Cependant, depuis leur lancement, ils ont aussi été utilisés pour faciliter des actes malveillants et criminels.

(Continue)

(a continué)

Des femmes ont trouvé des dispositifs qui ne leur appartenaient pas dans leur voiture et dans leurs affaires, ce qui les a fait craindre pour leur sécurité et leur a fait penser qu'ils pouvaient être utilisés à des fins de traquage (Willey, 2018; Suares, 2019; Ingram, 2021; Mac et Hill, 2021); des groupes de défense de la vie privée ont d'ailleurs exprimé des inquiétudes quant au traquage lorsque les AirTag ont été introduits (Mac et Hill, 2021). Les forces de l'ordre au Canada et aux États-Unis ont signalé que les AirTag sont également utilisés pour suivre et voler des voitures, et elles avertissent que ces dispositifs représentent un danger pour les victimes potentielles de violence conjugale (Mac et Hill, 2021; Tsekouras, 2021). Alors que les iPhone et les téléphones Android peuvent parfois être équipés de façon à avertir leur propriétaire lorsqu'un dispositif de repérage inconnu se trouve régulièrement à proximité (Samsung, 2021; Apple, 2022; Tile, 2022), plusieurs victimes et survivants ont affirmé craindre que les forces de l'ordre ne prennent pas toujours au sérieux les déclarations de notifications téléphoniques (Mac et Hill, 2021). En 2022, Apple a annoncé son intention d'introduire des fonctions supplémentaires, notamment des outils permettant aux « destinataires d'une alerte de suivi non désirée de localiser avec précision un AirTag inconnu » [traduction libre] (Apple, 2022). Jusqu'à présent, rien n'indique que les gouvernements du Canada ou des États-Unis aient tenté de réglementer les dispositifs de traçage.

La criminalisation n'est pas toujours une réponse efficace au harcèlement et aux abus en ligne

Des études ont révélé que la police hésite souvent à engager des poursuites pénales en cas de cyberintimidation. Lors d'entrevues ciblées avec 12 policiers canadiens, ceux-ci se sont montrés réticents à l'idée d'utiliser leurs ressources déjà limitées pour surveiller l'intimidation et le discours en ligne, tout en exprimant des inquiétudes quant à l'augmentation des poursuites criminelles contre les jeunes qui résulterait inévitablement de la criminalisation de la cyberintimidation. La police a affirmé sa conviction que les lois actuelles étaient suffisantes et efficaces pour délimiter la frontière entre les comportements en ligne criminels et non criminels (Broll et Huey, 2015). Des mises en garde contre la criminalisation de la cyberintimidation ont également été formulées dans une étude australienne de Pennell *et al.* (2022), qui a constaté que la criminalisation de ce comportement aura probablement peu d'impact sur les jeunes, dont beaucoup s'adonnent à la cyberintimidation après avoir eux-mêmes été cyberintimidés. Pennell *et al.* (2022)

avancent qu'une approche juridique de la cyberintimidation peut inutilement compromettre l'avenir d'un jeune, alors qu'une démarche éducative serait une solution plus adéquate.

Les policiers interrogés par Broll et Huey (2015) ont fait part de leur préférence pour des mesures moins punitives que les sanctions criminelles, et pour la recherche de solutions préventives aux côtés des personnes-ressources des écoles et des autres parties concernées. Les chercheurs dans ce domaine ont également recommandé des solutions axées sur la prévention et l'intervention précoce. En ce qui concerne particulièrement l'intimidation des jeunes LGBTIQ+, Abreu et Kenny (2018) recommandent des programmes de prévention et d'intervention spécialement adaptés aux besoins et aux problèmes. Les auteurs citent les programmes d'éducation par les pairs, les forums en ligne administrés par les écoles à l'intention des élèves susceptibles d'être victimes de cyberintimidation, les canaux de signalement anonyme des actes d'intimidation, les politiques scolaires explicites portant sur la cyberintimidation et le ciblage de groupes donnés, et la formation du personnel scolaire aux signes et aux conséquences de la cyberintimidation (Blumenfeld et Cooper, 2010; Hillier *et al*., 2010; Abreu et Kenny, 2018). Selon les données probantes, ce sont les approches globales — celles qui incluent les parents, les écoles et d'autres partenaires communautaires (encadré 3.3) — qui se sont révélées les plus efficaces pour réduire la cyberintimidation chez les jeunes (Couvillon et Ilieva, 2011; Bailey, 2015; Abreu et Kenny, 2018).

Encadré 3.3 Actions communautaires et crimes cyberfacilités

Les volontaires civils — qu'il s'agisse d'individus ou de groupes coordonnés à divers degrés — peuvent jouer un rôle actif dans la lutte contre la cybercriminalité (Huey *et al.*, 2013; Chang *et al.*, 2018). Il existe un large éventail de ces types d'actions, notamment le recueil de renseignements numériques sur les auteurs présumés de cybermenaces et leur transmission aux forces de l'ordre, le dénigrement en ligne des actes préjudiciables, l'autosurveillance du contenu dans les forums sur le Web et le vigilantisme en ligne (Huey *et al.*, 2013; Seering *et al.*, 2019; Loveluck, 2020). Il existe des exemples documentés de preuves recueillies par des groupes de bénévoles en partenariat avec les forces de l'ordre, qui ont conduit à l'arrestation et à la condamnation de personnes ayant commis des abus sexuels en ligne sur des enfants (Huey *et al.*, 2013) et de modération de contenu par les utilisateurs

(Continue)

(a continué)

contribuant au développement positif des communautés sur Internet (Seering *et al.*, 2019). Si la participation de volontaires civils au maintien de l'ordre en ligne peut être bénéfique dans certains cas, les forces de l'ordre considèrent souvent la participation communautaire comme inutile ou indésirable, sauf pour fournir des conseils (Huey *et al.*, 2013; Chang *et al.*, 2018). Elles s'inquiètent notamment de la question de la responsabilité juridique, de la sécurité des bénévoles, du respect de la vie privée des personnes soupçonnées d'avoir commis des cybercrimes et de l'érosion perçue de la confiance dans les forces de l'ordre (Huey *et al.*, 2013; Chang *et al.*, 2018).

Les données probantes indiquent que davantage de formation est nécessaire pour aider les professionnels concernés à détecter les façons d'utiliser la technologie pour faciliter la violence fondée sur le sexe, en particulier dans le cadre des relations conjugales. La formation des membres des services de police, des professionnels du droit et des travailleurs de soutien peut être un important élément de réflexion à l'avenir (Siminovic, 2017; Khoo *et al.*, 2019). En outre, la loi n'est qu'un élément parmi d'autres de la lutte contre ce type de harcèlement en ligne. En plus des mesures juridiques concernant la culpabilité des auteurs, les experts affirment que la responsabilité d'entreprise des fournisseurs de services et des platesformes de médias sociaux, notamment leurs politiques de modération du contenu et les directives communautaires, joue également un rôle crucial dans la réduction du harcèlement ainsi que dans la surveillance et l'élimination du contenu injurieux (Henry et Powell, 2016).

3.2 Technologies numériques et contenu répréhensible (terrorisme et propagande haineuse)

Dans cette section, nous abordons le contenu répréhensible qui, selon le NACCC, relève de la catégorie distincte de *terrorisme et de propagande haineuse*. Cette catégorie comprend la diffusion de contenu « ayant trait au racisme, à la xénophobie ou à l'incitation à la violence » [traduction libre] (NACCC, 2021a). La diffusion de ce contenu est préjudiciable et parfois considérée comme étant de nature criminelle — bien que, dans certaines circonstances, il soit difficile d'établir à quel moment un contenu haineux devient illégal. Pour donner lieu à des poursuites en vertu du droit criminel, le discours haineux doit répondre à certains critères établis dans le *Code criminel*, comme consister en de la communication publique de déclarations incitant à la haine contre un « groupe identifiable » qui est « susceptible d'entraîner une violation de la paix » (GC, 1985). Les données probantes portent à croire que

certaines formes de contenu répréhensible sont plus efficacement traitées par des moyens non criminels et le comité d'experts ne plaide pas en faveur de la criminalisation de tous les actes préjudiciables de la sorte.

3.2.1 Terrorisme (radicalisation et contenu extrémiste)

L'extrémisme violent peut être défini comme le recours à « la violence pour atteindre des objectifs idéologiques, religieux ou politiques extrêmes » (CCECPV, 2018). Si les extrémismes violents à caractère politique et religieux sont motivés par des ensembles particuliers de croyances politiques ou religieuses, les cibles de l'extrémisme violent à caractère idéologique (EVCI) varient considérablement (SCRS, 2021a). L'EVCI comprend la violence xénophobe (qui vise des groupes raciaux ou ethniques), la violence sexiste (qui vise les femmes et la communauté LGBTIQ+) ou la violence contre l'autorité (qui vise le gouvernement ou les forces de l'ordre).

En général, la radicalisation vers l'extrémisme et la violence est motivée par plusieurs facteurs comportementaux, historiques et sociétaux, notamment les réseaux sociaux d'un individu, ses griefs, ses vulnérabilités, son désir d'appartenance, son penchant pour la violence et son isolement (CCECPV, 2018). La pandémie de COVID-19 a exacerbé les facteurs généralement à la base de l'extrémisme, tels que l'isolement social, l'impression que le gouvernement va trop loin et le ralentissement économique. De nombreux groupes extrémistes ont exploité la pandémie pour diffuser des récits soutenant leur propre idéologie (Paikin, 2020; SCRS, 2021a). Contrairement aux individus motivés par l'extrémisme violent à caractère politique ou religieux, ceux qui sont motivés par l'EVCI agissent généralement de leur propre chef et ne sont pas affiliés à des groupes ou à des organisations, bien qu'ils puissent être influencés par des communautés en ligne (SCRS, 2021a).

L'environnement numérique est lié à la radicalisation

Bien que l'extrémisme violent ne soit pas principalement ancré dans les contextes numériques et que les TIC n'entraînent pas à elles seules la radicalisation des gens, certaines données montrent que l'exposition à du contenu extrémiste en ligne pourrait conduire à une radicalisation politique, religieuse ou autre, ou l'accélérer (Mullins, 2013; CCECPV, 2018; Hassan *et al.*, 2018; SECU, 2022a). De nombreux groupes extrémistes utilisent des outils tels que les applications de messagerie chiffrée, les platesformes de partage de médias et les principaux réseaux sociaux comme Facebook, Twitter et YouTube (SP, 2019a; hart *et al.*, 2021; Moonshot CVE, 2021). Des études sur l'extrémisme de droite et le djihadisme au Canada ont révélé qu'Internet facilitait la radicalisation parce qu'il permettait un accès facile à du

contenu extrémiste et à un réseau d'individus partageant les mêmes idées (Mullins, 2013; Gaudette *et al.*, 2020; Dawson et Amarasingam, 2021).

La participation à des discussions en ligne, par le biais de forums, de clavardoirs et de platesformes de médias sociaux, permet aux gens de s'immerger dans du contenu et des réseaux extrémistes violents (Gaudette *et al.*, 2020). Les médias sociaux ont, dans certains cas, une plus grande influence sur les processus de radicalisation que les groupes de connaissances en personne, les amis, la famille ou les chefs religieux (Bastug *et al.*, 2020). L'immersion dans des environnements numériques est un élément susceptible de renforcer les croyances et l'affirmation idéologique (Perry et Scrivens, 2016; Selim, 2019). Des schémas similaires ont été constatés dans des groupes Facebook d'extrême droite au Québec, qui pratiquent le vigilantisme numérique (Tanner et Campana, 2020). Une étude du contenu de *Stormfront Canada*, l'un des forums Web les plus visités par les extrémistes de droite, a révélé que le volume, la gravité et la durée du contenu antisémite, anti-noir et anti-LGBTIQ+ affiché par ses utilisateurs ont augmenté en 15 ans, ce qui révèle une radicalisation accrue (Scrivens *et al.*, 2020).

Les groupes extrémistes communiquent et recrutent au moyen des médias sociaux

Les TIC offrent des platesformes permettant à des individus de recruter d'autres personnes pour leur cause, de transmettre de la propagande et de communiquer sur des attaques et de les planifier (CCECPV, 2018; SP, 2019a). La plupart des gens ayant des opinions extrémistes ne sont pas affiliés à des groupes criminels organisés; cependant, les forums en ligne permettent aux extrémistes isolés d'étendre leur portée et « d'être plus actifs dans les campagnes virtuelles de recrutement idéologique et de radicalisation » [traduction libre] (Selim, 2019), en partie en facilitant la publication et la diffusion de matériel extrémiste (Perry et Scrivens, 2016). Les médias sociaux permettent aux extrémistes d'identifier des groupes particuliers et de les cibler à des fins de recrutement avec du matériel et des messages personnalisés (CCECPV, 2018). Les groupes extrémistes utilisent également des tactiques d'accroche telles que l'humour, les mèmes et les jeux vidéo pour cibler les jeunes (encadré 3.4), ce qui est préoccupant compte tenu du nombre croissant de jeunes en voie de radicalisation (Ahmad, 2017; ASIO, 2021).

Encadré 3.4 Utilisation de l'humour, des mèmes et des jeux vidéo par les groupes extrémistes

L'humour est un moyen efficace d'attirer les gens vers les idéologies extrémistes. Un document que l'on présume être un guide de style destiné aux rédacteurs potentiels d'un blogue néonazi connu encourage les auteurs à utiliser l'humour comme méthode de diffusion de leur contenu haineux (Feinberg, 2017). Présenter des idées haineuses en ligne sous le couvert de l'humour, de la satire ou de la parodie offre la protection du déni plausible selon lequel « si l'auteur n'indique pas ses intentions, il peut être difficile de distinguer entre [...] l'extrémisme et une parodie d'extrémisme » (Greene, 2019). Les groupes extrémistes utilisent de plus en plus ces tactiques pour diffuser des messages et recruter de nouveaux adeptes (Donovan, 2019; Greene, 2019); l'humour permet aux organisations néonazies de publier des œuvres haineuses sous couvert de faciliter la camaraderie, le plaisir ou l'amusement, ce qui est particulièrement utile pour attirer un public jeune (Askanius, 2021).

L'humour et les mèmes peuvent également être utilisés pour promouvoir un récit du type « nous contre eux » en déshumanisant et en tournant à la légère les luttes des personnes extérieures à sa sous-culture (Greene, 2019; Mortensen et Neumayer, 2021). La culture des mèmes, qui consiste à réarranger et à s'approprier des éléments médiatiques connus, exploite la familiarité du matériel source et provoque un choc en subvertissant les attentes du spectateur (Greene, 2019). Pour établir une véritable connexion avec le support, ce dernier doit maîtriser la sousculture et les blagues d'initiés du groupe. Ainsi, les créateurs de mèmes peuvent adapter leur message afin qu'il résonne auprès de leur public cible grâce à l'humour et à la connaissance de la culture Internet (Marwick et Lewis, 2017).

Les jeux vidéo multijoueurs en ligne facilitent également le recrutement de jeunes par les groupes extrémistes, la diffusion de la propagande et la communication interactive au sein de ces mêmes groupes (Robinson et Whittaker, 2020). La boutique en ligne et la fonction de clavardage internes à Twitch, un service populaire de diffusion en continu en direct destiné aux développeurs et aux joueurs de jeux vidéo, ont toutes deux été utilisées par des extrémistes pour promouvoir facilement leur contenu auprès d'un large public (O'Connor, 2021). Twitch enregistre en moyenne environ 30 millions de visiteurs chaque jour, dont près de la moitié sont âgés de 18 à 34 ans (O'Connor, 2021). Les influenceurs d'extrême droite et les théoriciens du complot ont gagné des milliers de dollars en diffusant de la mésinformation et du contenu extrémiste sur cette plateforme (Browning, 2021).

Bien qu'Internet permette aux organisations d'extrême droite de communiquer au-delà des frontières, la majeure partie du contenu extrémiste qui circule au Canada provient de l'intérieur du pays

Au Canada, on a constaté une augmentation de la menace animée par « le genre, la xénophobie, l'opposition à l'autorité et d'autres motifs fondés sur des récriminations personnelles » (SCRS, 2022). Les communautés canadiennes de la sécurité nationale et du contre-terrorisme concentrent leurs activités de surveillance sur les groupes nationalistes d'extrême droite et sur les groupes de suprémacistes blancs (Crosby, 2021). La portée mondiale d'Internet fait en sorte que des personnes de partout au Canada peuvent accéder à des communautés radicales en ligne (Moonshot CVE, 2021), et les extrémistes de droite réseautent et coopèrent de plus en plus au-delà des frontières (Musharbash, 2021). De nombreuses organisations d'extrême droite au Canada ont des liens directs avec des groupes similaires aux États-Unis et en Europe (Perry et Scrivens, 2016) et le contenu de l'extrême droite canadienne est influencé par les événements survenant aux États-Unis (Hart *et al.*, 2021). Cependant, la majeure partie du contenu extrémiste qui circule au Canada provient du Canada même (Hart *et al.*, 2021; SECU, 2022a). L'extrémisme est un problème qui se produit à l'intérieur du Canada, et non un problème qui est uniquement importé au pays.

Le volume d'activités d'extrême droite en ligne est cependant faible par rapport à l'ensemble de l'utilisation des médias sociaux au Canada en général : on recense une page ou un groupe d'extrême droite actif pour 235 420 utilisateurs de Facebook (Hart *et al.*, 2021). Cela dit, une analyse a répertorié 2 467 comptes, pages et canaux actifs proposant du contenu d'extrême droite au Canada qui, collectivement, ont créé en moyenne plus de 60 000 éléments de contenu uniques chaque semaine (Hart *et al.*, 2021). En 2020, ce contenu a produit environ 44 millions de réactions sur Facebook et plus d'un demi-million de commentaires sur YouTube, a été repartagé sur Twitter près de 9 millions de fois et a été visionné plus de 16 millions de fois sur Telegram (Hart *et al.*, 2021).

Certains éléments de contenu extrémistes en ligne incitent à la violence

Une partie du contenu extrémiste, mais pas la totalité, est considéré comme criminel. À titre d'exemple, environ 31 000 des 3 millions d'éléments de contenu d'extrême droite analysés au Canada utilisaient « un langage répréhensible, agressif, déshumanisant ou violent visant une personne ou un groupe de personnes » [traduction libre], et comprenaient des appels à la violence (Hart *et al.*, 2021). La violence est un élément commun aux cercles extrémistes canadiens, étant donné que leurs membres partagent souvent des guides sur la préparation à

celle-ci (Hart *et al.*, 2021), qui incluent des mots qui se rapportent à la violence et contiennent plus de mentions de violence mortelle par arme à feu que du contenu similaire provenant d'Australie (Hutchinson *et al.*, 2021). La publication puis la diffusion en ligne de manifestes extrémistes dans un pays peuvent également inspirer des actes extrémistes violents hors ligne dans d'autres pays (Berger, 2019).

Les jeunes hommes sont les plus susceptibles de rechercher du contenu extrémiste en ligne

On dispose de certaines données sur les caractéristiques démographiques des personnes qui recherchent du contenu extrémiste au Canada. Par exemple, Moonshot CVE (2021) a recensé 171 382 recherches sur Google au Canada entre février 2019 et mars 2020 au moyen de mots-clés correspondant à Daesh, Al-Qaïda et à du contenu d'extrême droite qui incite à la violence et promeut des théories du complot. Une analyse ultérieure a relevé que du contenu extrémiste de tous les spectres idéologiques, religieux et politiques est recherché en ligne partout au Canada. Notamment, les utilisateurs âgés de 25 à 34 ans étaient les plus susceptibles de rechercher ce type de contenu (près de 30 % des recherches) et dans environ 75 % des cas, il s'agissait d'hommes (Moonshot CVE, 2021).

3.2.2 Propagande haineuse

Comme dans le cas du harcèlement en ligne, il peut être difficile de définir le point où le contenu haineux passe du statut d'abominable (mais légal) à celui d'illégal. Le discours haineux (appelé *propagande haineuse* dans le *Code criminel*) est illégal au Canada (GC, 1985). L'apologie du génocide, l'incitation à la haine contre un « groupe identifiable » qui est « susceptible d'entraîner une violation de la paix » et les communications qui « encouragent volontairement la haine contre un groupe identifiable » [traduction libre] dans un lieu public sont des infractions criminelles (GC, 1985; Walker, 2018). Le terme « groupe identifiable » peut renvoyer à la religion, à l'ethnie, à l'identité de genre, à la sexualité ou à la race. L'article 320 du *Code criminel* permet de saisir le matériel de propagande haineuse, y compris les données informatiques, sur ordre du tribunal et du procureur général (GC, 1985). Les accusations en vertu des articles 318 et 319 sont principalement utilisées dans les cas où une personne en incite d'autres à la haine, et nécessitent le consentement du procureur général — un processus long qui peut parfois prolonger la durée des enquêtes (Corb, 2015; Proctor, 2020).

De nombreux incidents susceptibles d'inclure des actes haineux peuvent mener à des poursuites pour d'autres infractions, comme voies de fait ou harcèlement, la haine étant considérée comme une circonstance aggravante lors de la détermination de la peine (Walker, 2018; Proctor, 2020). Il n'existe pas de définition écrite de la *haine* dans le *Code criminel* du Canada, mais une définition a

été proposée dans le Projet de loi C-36 (2021) (chapitre 5); les cas de propagande haineuse au Canada ont donné lieu à une interprétation juridique de la *haine* qui renvoie à « des émotions exceptionnellement fortes et profondes de détestation se traduisant par des calomnies et la diffamation » (CSC, 1990a) à l'égard d'un groupe cible et qui nie le respect et la dignité envers les cibles (CSC, 1990b).

Les crimes haineux en ligne semblent être en hausse, mais ils sont sous-déclarés

Il est difficile, et probablement impossible, d'obtenir des renseignements complets et précis sur les incidences du discours haineux en ligne (Gill, 2020). Cela dit, Statistique Canada a rapporté 572 cybercrimes motivés par la haine enregistrés par la police entre 2010 et 2019 (Moreau, 2021b). On sait que ce chiffre constitue un sous-dénombrement étant donné que la Police provinciale de l'Ontario (OPP) n'a pas publié d'indicateur de cybercriminalité de 2010 à 2018 et que plusieurs autres services de police municipaux n'ont pas été en mesure de le faire pour plusieurs années au cours de cette même période. Parmi les cybercrimes motivés par la haine qui ont été signalés, la profération de menaces (38 %) était le type de cybercrime haineux le plus courant entre 2010 et 2019, suivi de l'incitation publique à la haine (17 %), des communications indécentes ou harcelantes en ligne (17 %) et du harcèlement criminel (12 %) (Moreau, 2021b).

Les entreprises exploitant des platesformes de médias sociaux ont également fourni des instantanés de la prévalence du discours haineux en ligne. Par exemple, au cours d'une période de trois mois allant de juillet à septembre 2021, Meta aurait pris des mesures contre 22,3 millions de cas de discours haineux sur Facebook (Facebook - Meta Transparency Center, 2021); entre avril et juin 2021, YouTube a pris des mesures contre 57,8 millions de commentaires qualifiés de « haineux ou répréhensibles » et a supprimé 42 013 chaînes pour la même raison au cours de cette même période (Google, 2021). Cependant, le contenu haineux n'est pas toujours supprimé rapidement (JUST, 2019), les comptes qui propagent du contenu haineux peuvent réapparaître après avoir été supprimés (Velásquez *et al.*, 2021) et le contenu supprimé peut ne pas être uniforme d'une plateforme à l'autre (chapitre 4).

Les contenus haineux peuvent toucher un large public en ligne

Si le discours haineux était autrefois diffusé par courrier, brochures ou supports audiovisuels tels que les cassettes vidéo, les DVD et les CD, l'adoption généralisée des TIC a fourni de nouvelles platesformes permettant aux individus de répandre du contenu haineux en ligne. Les TIC sont généralement plus efficaces pour atteindre des publics larges avec moins d'efforts que les méthodes antérieures, fondées sur l'analogie (Rohlfing, 2015). La communication et la propagation du

discours haineux varient en fonction des technologies utilisées, le contenu hébergé sur des platesformes comme Telegram ou 4chan, où le contrôle est moins strict, contenant plus souvent des insultes que le contenu publié sur des platesformes telles que Facebook (Hart *et al.*, 2021).

Le contenu haineux peut passer d'une plateforme de médias sociaux à l'autre, ce qui rend son contrôle difficile

Même des politiques de modération du contenu rigoureuses peuvent ne pas être efficaces pour empêcher la propagation du discours haineux, car les utilisateurs qui lisent ce contenu le font souvent sur plusieurs platesformes. Une étude portant sur la propagation de matériel malveillant sur la COVID-19 parmi les communautés haineuses numériques a révélé que les platesformes moins modérées (p. ex. 4chan) ont une influence sur la capacité des platesformes conventionnelles (p. ex. Facebook) à modérer le contenu haineux, parce que les premières permettent la propagation rapide de matériel malveillant d'une plateforme à l'autre par l'entremise de communautés haineuses interconnectées (Velásquez *et al.*, 2021). Les auteurs notent que « les activités malveillantes peuvent sembler isolées et largement éradiquées sur une plateforme donnée, alors qu'en réalité elles se sont déplacées vers une autre. Là, le contenu malveillant peut s'épanouir hors du contrôle de la plateforme d'origine, être affiné, puis *réintroduit dans la plateforme d'origine* à l'aide d'un lien dans le sens inverse » [traduction libre]. Autrement dit, les gens peuvent être dirigés de sites modérés vers des sites moins modérés au moyen d'un hyperlien, ce qui a pour effet qu'« un utilisateur d'une communauté de médias sociaux grand public, comme un enfant qui se connecte à d'autres pour jouer en ligne ou un parent qui cherche des informations sur la COVID-19, ne se trouve qu'à quelques liens de contenu intensément haineux » [traduction libre] (Velásquez *et al.*, 2021). Le manque d'uniformité des politiques de modération du contenu sur les différentes platesformes facilite la migration des utilisateurs extrémistes et sans plateforme d'appartenance vers des espaces numériques alternatifs, où ils diffusent du contenu haineux (Rogers, 2020).

Les événements hors ligne influencent la fréquence et le type du discours haineux apparaissant en ligne

De plus en plus de données probantes indiquent une corrélation entre les événements externes et l'augmentation du discours haineux en ligne. Par exemple, une étude de 2018 qui a surveillé les messages diffusés sur Twitter et Reddit a constaté une augmentation du discours haineux contre les communautés arabes et musulmanes à la suite d'attaques perpétrées par ou contre des Arabes ou des musulmans dans des pays où ils constituent des groupes minoritaires (Olteanu *et al.*, 2018). Ces résultats concordent avec d'autres études qui ont examiné la

prolifération de la haine en ligne à la suite de ce qui est décrit comme des « événements déclencheurs » (Awan et Zempi, 2015; Benesch *et al.*, 2016; Faris *et al.*, 2016). La COVID-19, qui a été l'un de ces événements, a conduit à une hausse des crimes et du discours haineux contre les communautés asiatiques partout dans le monde (Macguire, 2020). Sur Internet, le suivi de ce phénomène a été effectué au moyen de la prévalence d'un langage désobligeant et raciste, certains individus semblant rejeter la responsabilité de la pandémie sur les communautés et les pays asiatiques (Macguire, 2020).

Même en l'absence d'événement déclencheur, de nouvelles données probantes indiquent un lien entre la haine en ligne et la victimisation hors ligne. Une étude britannique, qui s'est appuyée sur des données obtenues auprès de la Police métropolitaine de Londres et sur des messages publiés dans les médias sociaux, a révélé « une association positive entre le discours haineux sur Twitter ciblant la race et la religion et les infractions aggravées par des motifs raciaux et religieux hors ligne à Londres » [traduction libre] (Williams *et al.*, 2020). Les auteurs de l'étude ont décrit les médias sociaux comme jouant un rôle « non négligeable » dans la facilitation des attaques hors ligne et un rôle important dans la formule générale qui inspire les crimes haineux. Cette formule inclut d'autres facteurs connus tels que le contexte historique, politique, social et géographique (Williams *et al.*, 2020). L'étude confirme les constatations d'autres études qui établissent un lien entre les crimes haineux hors ligne contre les musulmans aux États-Unis et l'activité incendiaire de Donald Trump sur Twitter pendant sa campagne présidentielle (Müller et Schwarz, 2020a) et entre le discours haineux en ligne et les incidents violents contre les communautés de réfugiés et d'immigrés en Allemagne (Müller et Schwarz, 2020b). Dans l'ensemble, ces éléments indiquent que les communautés communément ciblées pourraient s'attendre (et se préparer) à un possible harcèlement en ligne avant des événements majeurs ou mettre sur pied des plans pour réagir face à des événements déclencheurs inattendus.

Les communautés marginalisées et minorisées risquent davantage d'être victimes de la haine en ligne

Une enquête réalisée en 2021 a révélé que 47 % des personnes utilisant Internet au Canada ont vu ou subi des commentaires ou du contenu racistes en ligne, 38 % ont vu ou subi des commentaires ou du contenu homophobes et 30 % ont vu ou subi des commentaires ou du contenu sexistes (Abacus Data, 2021). Les personnes racisées et les jeunes au Canada sont plus susceptibles de tomber sur les types de contenu mentionnés précédemment sur les platesformes principales telles que Facebook et YouTube (Andrey *et al.*, 2021a). Parmi les cybercrimes motivés par la haine signalés à la police au pays entre 2010 et 2019, les personnes étaient le plus

souvent ciblées parce qu'elles étaient musulmanes (17 %) ou juives (13 %), en raison de leur orientation sexuelle (13 %) ou parce qu'elles étaient noires (10 %) (Moreau, 2021b).

Lors d'une autre enquête menée en 2021 auprès de 2 500 personnes âgées de 16 ans ou plus et représentant un échantillon ethnique du Canada, 26 % des répondants ont déclaré recevoir des messages haineux sur des applications de messagerie privée (p. ex. Facebook Messenger, WhatsApp, Snapchat) au moins une fois par mois (Andrey *et al.*, 2021a). Le taux augmente considérablement lorsqu'on sélectionne les personnes de couleur (p. ex. il passe à 58 % pour les Latino-Américains, à 44 % pour les Moyen-Orientaux et à 44 % pour les Asiatiques du Sud-Est). Les platesformes sur lesquelles les messages ont été envoyés avaient des politiques de contenu interdisant le discours haineux et permettant aux utilisateurs de signaler la réception de messages nuisibles (Andrey *et al.*, 2021a). Malgré ces politiques et les fonctions des platesformes, les messages étaient toujours émis et reçus et pouvaient donc causer des préjudices même s'il existait un moyen de les signaler ou de les traiter après leur réception.

3.3 Technologies numériques et fraude

La *fraude*, au sens large, est définie par le NACCC comme « la perte de biens (y compris de données) causée dans l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour soi-même ou pour une autre personne » [traduction libre] (NACCC, 2021a). Cependant, sa nature est en train de changer. Les campagnes de fraude peuvent utiliser les TIC pour s'adapter rapidement aux événements du moment, comme les élections, la déclaration des revenus, les nouvelles ou les crises sanitaires mondiales telles que la pandémie de COVID-19 (Centre canadien pour la cybersécurité, 2020a). Il en résulte que certains types de cyberfraude et de tentatives d'extorsion connexes sont plus évoluées, en partie parce que les places de marché de la cybercriminalité comme le Web clandestin laissent des acteurs relativement peu avertis acheter les outils et les services nécessaires pour mener à bien des campagnes de fraude en ligne (Centre canadien pour la cybersécurité, 2020a) (section 4.2).

D'autres formes de cyberfraude ne sont peut-être pas perfectionnées sur le plan technologique (p. ex. les arnaques par SMS), mais elles peuvent causer des préjudices importants sans beaucoup d'efforts grâce aux médias sociaux (FTC, 2022). Les opérations frauduleuses se déroulent couramment dans plusieurs États, ce qui rend difficile ou presque impossible, dans certains cas, pour les forces de l'ordre d'enquêter sur les crimes et de porter des accusations contre les contrevenants (EDSC, 2019). Bien que le comité d'experts reconnaisse l'existence de multiples formes de cyberfraude, il s'est concentré sur celles qui incluent la

fausse représentation (p. ex. les escroqueries), tout en accordant une attention particulière aux pratiques prédatrices de fraude en ligne qui ciblent les communautés vulnérables, en raison des graves préjudices que ces pratiques peuvent causer.

3.3.1 Ampleur et répercussions de la cyberfraude

Bien que les obstacles au signalement persistent, la cyberfraude est le type de cybercriminalité le plus fréquemment signalé

Comme d'autres types de cybercrimes, la cyberfraude est sous-déclarée. Selon certaines estimations, « environ 5 % seulement des incidents de fraude sont signalés aux organismes d'application de la loi, ce qui rend la collecte de preuves et l'intervention difficiles » (EDSC, 2019). En même temps, la cyberfraude est le cybercrime le plus souvent signalé par la police au Canada et a augmenté de plus de 150 % depuis 2016 (StatCan, 2021b). Plus de 138 000 incidents de fraude ont été déclarés à la police au Canada en 2020 (Moreau, 2021a), dont près de 30 000 ont été classés comme de la cyberfraude (StatCan, 2021b). Le type de fraude le plus courant au Canada est l'extorsion (c.-à-d. l'obtention illégale d'argent, de biens ou de services d'une personne par la coercition), suivie de la fraude d'identité et de l'accès illégal à des renseignements personnels (Centre antifraude du Canada, 2021b).

En 2020, on a signalé au Canada plus de 17 000 incidents de fraude concernant l'extorsion, qui ont touché environ 6 700 personnes (Centre antifraude du Canada, 2021b). Les auteurs de cybermenaces menacent souvent de lancer des cyberattaques ou de voler (ou de prétendre avoir volé) des renseignements compromettants afin d'extorquer de l'argent à leurs victimes (Centre canadien pour la cybersécurité, 2020a). Certaines formes de fraude documentées au Canada comprennent l'utilisation de faux profils sur les médias sociaux et les sites de rencontre pour faciliter l'extorsion et la fraude (Centre canadien pour la cybersécurité, 2020b). Dans certains cas, les auteurs de cybermenaces ont accès à des vidéos intimes de leurs victimes et leur extorquent de l'argent en menaçant de les envoyer aux contacts de ces dernières (Centre canadien pour la cybersécurité, 2020a).

L'importance des déclarations de cyberfraude par rapport aux autres cybercrimes peut être due en partie au fait que le Canada dispose d'un mécanisme de signalement en ligne spécifique pour la cyberfraude (Centre antifraude du Canada, 2021a), contrairement aux autres formes de cybercriminalité. La fraude était également l'infraction la plus courante dans les affaires dévoilées par le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) en 2021 (CANAFE, 2021a).

La cyberfraude cause des préjudices financiers et psychologiques considérables

Les préjudices financiers découlant de la cyberfraude sont considérables et en augmentation. Selon le Centre antifraude du Canada, l'organe de signalement des fraudes et dépôt central de données sur les fraudes du gouvernement du Canada, plus de 67 000 personnes et entreprises au Canada ont été victimes de fraude en 2020, au cours de laquelle elles ont collectivement perdu plus de 104 millions de dollars (CAFC, 2021b). Ce montant a presque doublé l'année suivante, les pertes s'étant élevées à près de 200 millions de dollars entre janvier et octobre 2021 (CAFC, 2021c). Ce sont les fraudes dites de « stratagème de rencontre », souvent perpétrées en ligne, qui ont causé les plus grandes pertes financières aux individus au pays en 2020 (18,5 millions de dollars) (CAFC, 2021b). La pandémie de COVID-19 a offert un nouveau terrain pour commettre des fraudes; de mars 2020 à mai 2021, on a enregistré près de 20 000 victimes et 7,4 millions de dollars perdus au Canada en raison de fraudes liées à cette pandémie (p. ex. des escrocs demandant un paiement pour des conseils médicaux frauduleux) (Moreau, 2021a).

Les préjudices causés par la cyberfraude dépassent les pertes financières. Celle-ci a des conséquences émotionnelles et psychologiques sur les victimes et les survivants, elle provoque notamment des traumatismes qui, dans des cas extrêmes, ont été un facteur contribuant au décès par suicide (Cross *et al.*, 2016; Cross, 2017). Les autres préjudices documentés de la fraude en ligne comprennent la perte de sommeil, la peur permanente et l'inquiétude pour sa sécurité physique (Cross *et al.*, 2016).

Les institutions financières déploient des efforts considérables en prévention de la fraude lorsqu'elles sont touchées

Lorsque les pertes financières dues à la fraude frappent durement les institutions financières, de solides efforts pour prévenir d'autres fraudes ont tendance à suivre. Par exemple, la fraude par carte de crédit entraîne environ 800 millions de dollars de pertes financières annuelles au Canada (Henry *et al.*, 2018; Simple Rate, 2021), mais les politiques de protection Responsabilité zéro font que les institutions financières remboursent les transactions non autorisées aux clients victimes de la fraude (ACFC, 2019; ABC, 2022). Cela les a incitées à investir massivement dans la prévention. Entre 2009 et 2019, les six plus grandes banques du Canada ont collectivement consacré 100 milliards de dollars à la technologie, améliorant ainsi considérablement leur cybersécurité interne (ABC, 2022).

3.3.2 Effets de la cyberfraude sur certains groupes démographiques

Les personnes âgées sont vulnérables à la cyberfraude, qui leur inflige des pertes financières importantes

Au Canada, les personnes âgées sont particulièrement vulnérables à la cyberfraude. Le déclin de leurs capacités cognitives, comme la mémoire à court terme et la vigilance, est corrélé avec une plus grande vulnérabilité à la tromperie en ligne (Ebner *et al.*, 2020). L'isolement social et l'insécurité économique peuvent exacerber leur vulnérabilité (Cross, 2016; EDSC, 2019), tout comme leur faible niveau de littératie numérique, qui peut complexifier pour eux le discernement efficace des courriels authentiques par rapport aux courriels d'hameçonnage (Grilli *et al.*, 2021). Cependant, les attaques d'hameçonnage étant de plus en plus perfectionnées et trompeuses, elles sont difficiles à déceler, même avec une forte littératie numérique (Alkhalil *et al.*, 2021). La cyberfraude peut également être liée à l'abus et à l'exploitation des personnes âgées (JUS, 2010), pour lesquelles il existe des protections inscrites dans la législation sur la vie privée et les droits de la personne (encadré 3.5).

Encadré 3.5 Protections contre l'exploitation des personnes âgées

Toutes les provinces et tous les territoires canadiens possèdent une loi sur les droits de la personne qui protège contre la discrimination fondée sur l'âge (GC, 2021b). Cependant, le Québec a une approche plus large en matière de définition et de traitement de la question de la maltraitance des personnes âgées (GC, 2021b). La *Charte des droits et libertés de la personne* du Québec contient des dispositions spécifiques garantissant le droit des personnes âgées à être protégées contre toute forme d'exploitation (Gouv. du QC, 1976), qui attribue à cette protection un statut quasi constitutionnel (GC, 2021b). L'exploitation — qui peut être financière, physique ou émotionnelle — est le fait de profiter d'une personne vulnérable et de lui causer du tort (Éducaloi, 2022). La *Commission des droits de la personne et des droits de la jeunesse* du Québec possède une équipe spéciale qui mène des enquêtes sur l'exploitation des personnes âgées, les aide à trouver le soutien approprié et peut demander à un tribunal d'ordonner une mesure d'urgence (CDPDJ, 2022; Éducaloi, 2022). L'exploitation peut être signalée sans le consentement de la victime (CDPDJ, 2022).

(Continue)

(a continué)

L'exploitation financière des personnes âgées est la forme d'exploitation la plus déclarée à la Commission (CDPDJ, 2022) et l'exploitation rattachée à la fraude peut inclure l'obtention d'argent d'une personne âgée en utilisant la force ou des menaces (Éducaloi, 2022).

En 2015, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) a été modifiée pour permettre aux organisations de communiquer avec une institution gouvernementale ou avec le plus proche parent ou le représentant autorisé d'une personne si :

> *i. « l'organisation a des motifs raisonnables de croire que l'intéressé a été, est ou pourrait être victime d'exploitation financière »,*
>
> *ii. la communication est faite uniquement à des fins liées à la prévention de l'exploitation à une enquête y ayant trait,*
>
> *iii. il est raisonnable de s'attendre à ce que la communication effectuée au su ou avec le consentement de l'intéressé compromettrait la capacité de prévenir l'exploitation ou d'enquêter sur celle-ci.* »

GC (2000a)

Cette modification a toutefois été critiquée comme étant discriminatoire à l'égard des personnes âgées et comme pouvant les exposer à des risques supplémentaires parce que, dans de nombreux cas, l'exploitation financière est perpétrée par le plus proche parent (Van Cauwenberghe, 2015).

Les types de fraude les plus courants subis par les adultes canadiens âgés de 60 ans et plus étaient l'extorsion, les arnaques concernant les services (y compris les services de soutien technique) et l'hameçonnage (EDSC, 2019). C'est la fraude dite de « stratagème de rencontre » qui a généré les pertes financières les plus importantes chez les adultes âgés (9 millions de dollars, soit 25 % de toutes les pertes dues aux stratagèmes de rencontre). Ces chiffres sont probablement sous-estimés, car les personnes âgées sont moins susceptibles de déclarer les fraudes à la police, en partie en raison d'un sentiment de honte et du « fait qu'elles considèrent qu'un signalement aura peu d'effet, particulièrement lorsque la valeur des pertes est faible » (EDSC, 2019).

Les arnaques et les pratiques d'usurpation d'identité visent souvent les nouveaux immigrants au Canada

Les nouveaux immigrants au Canada sont également plus vulnérables à la cyberfraude que la population générale (GRC, 2019; IRCC, 2021a). Les auteurs de cybermenaces se font souvent passer pour des organisations légitimes (p. ex. des organismes gouvernementaux ou des banques) et créent de faux sites Web et de fausses publicités en ligne (CAFC, 2021d). Ces sites et annonces prétendent souvent offrir des services d'immigration peu coûteux ou garantissent faussement un emploi aux nouveaux immigrants en échange de frais (Centre canadien pour la cybersécurité, 2020a). Plus de 3 500 faux comptes de médias sociaux, sites Web et serveurs de messagerie du gouvernement du Canada ont été démantelés en 2020 (Centre canadien pour la cybersécurité, 2020a).

Un autre type courant de cyberfraude touchant les nouveaux immigrants consiste à se faire passer pour un fonctionnaire de l'immigration en ligne ou au téléphone et de menacer d'arrêter ou d'expulser sa cible à moins qu'elle ne paie des frais ou ne donne des renseignements personnels (IRCC, 2021b). Ces arnaques sont parfois facilitées par l'usurpation de numéros de téléphone[7], une pratique qui n'est pas illégale (CAFC, 2020; Daubs, 2022). Bien que le CRTC dispose de certaines règles sur les télécommunications non sollicitées, les outils réglementaires et de droit civil pour combattre l'usurpation d'identité au Canada sont plus limités que dans d'autres pays comme les États-Unis (Daubs, 2022).

Les jeunes adultes sont plus susceptibles que les plus vieux de se faire arnaquer sur les médias sociaux

Les escrocs utilisent les médias sociaux pour atteindre les gens et commettre des fraudes. Aux États-Unis, la cyberfraude signalée a augmenté dans chaque groupe d'âge en 2021, mais les personnes âgées de « 18 à 39 ans étaient plus de deux fois plus susceptibles que les adultes plus âgés de déclarer avoir perdu de l'argent » [traduction libre] à cause d'arnaques sur les médias sociaux (FTC, 2022). Bien qu'aucune donnée équivalente ne soit disponible au Canada, les jeunes utilisent fortement les médias sociaux au Canada et les données probantes montrent que les escrocs s'en servent de plus en plus pour cibler différents groupes démographiques, y compris les jeunes (GRC, 2018; Centre canadien pour la cybersécurité, 2020b). Face à ce phénomène, Facebook Messenger a introduit des avis de sécurité qui apparaissent dans les clavardages et sont accompagnés de ressources visant à aider les gens à déceler les activités suspectes, y compris les arnaques (Facebook, 2020a).

7 L'usurpation consiste pour un appelant à manipuler délibérément l'information transmise sur l'afficheur afin de dissimuler son identité.

3.4 Résumé

Pour répondre à la question du commanditaire sur la façon dont les activités criminelles graves et les comportements préjudiciables ont évolué pour exploiter les progrès des TIC, le comité d'experts s'est penché sur l'exploitation, le harcèlement et la maltraitance, sur les activités extrémistes violentes, sur la propagation de la haine et sur la fraude. Ce chapitre a notamment décrit comment les TIC pouvaient étendre le champ d'action des auteurs de cybermenaces en leur permettant de recruter et de communiquer plus facilement entre eux, et de trouver et de cibler des victimes. Cela crée de nombreux défis pour les autorités qui cherchent à prévenir et contrer les activités préjudiciables, et à enquêter à leur sujet, au moyen d'outils ou de méthodes qui peuvent être inadaptés à des contextes numériques en constante évolution.

Les actes préjudiciables se situent sur un spectre de criminalité et de légalité. Selon le cas, certains actes communément considérés comme répréhensibles, tels que la cyberintimidation, le harcèlement en ligne ou la diffusion d'hypertrucages, peuvent ne pas être criminels ou même illégaux. Cependant, il est prouvé que ces cyberméfaits ainsi que d'autres peuvent avoir des conséquences physiques, psychologiques et financières considérables sur les personnes visées. Dans un même temps, tout le monde ne court pas le même risque d'être victime de méfaits en ligne. Les cibles courantes d'actes et de contenu préjudiciables sur Internet sont les femmes, les jeunes, les communautés racisées et minoritaires et certaines professions comme le journalisme, ce qui souligne la nature intersectionnelle de ce problème.

Pour lutter contre ces méfaits, il faut combiner des approches juridiques et non juridiques fondées sur l'expérience des victimes et des survivants. Le comité d'experts a constaté que les réformes juridiques peuvent parfois limiter la diffusion d'hypertrucages et la diffusion non consensuelle de contenu intime. La criminalisation de tous les cas de cyberintimidation n'est toutefois pas souhaitable pour tout un ensemble de raisons, notamment l'impact négatif sur les jeunes, dont beaucoup se livrent à la cyberintimidation après avoir eux-mêmes vécu une expérience traumatisante. Parmi les autres approches possibles pour lutter contre les cyberméfaits, citons les programmes éducatifs, les directives communautaires et les programmes de modération du contenu sur les platesformes de médias sociaux, ainsi que les mesures de prévention de la fraude mises en place par les banques. Cependant, il n'existe pas de solution facile ou universelle au problème des cyberméfaits; toutes les solutions qui existent actuellement peuvent être contournées ou devenir désuètes en raison de la nature évolutive des TIC.

Le chapitre suivant approfondit ces difficultés en examinant comment des outils et des forums numériques spécifiques, notamment concernant les cryptomonnaies et la mésinformation en ligne, compliquent les efforts d'endiguement et d'application de la loi en contribuant à dissimuler, à financer et à amplifier les actes préjudiciables. L'utilisation de ces outils a conduit le secteur privé, y compris les entreprises de médias sociaux, à jouer un rôle de plus en plus actif et à davantage s'autoréguler dans la gestion des actes préjudiciables et dans la modération du contenu préjudiciable.

4

Facilitateurs numériques des méfaits

Constatations du chapitre

- Les sites de sociofinancement, les cryptomonnaies et le Web clandestin sont peu surveillés, peuvent être utilisés pour financer et dissimuler des actes préjudiciables en ligne et rendre les lois difficiles à appliquer.
- Le Web clandestin offre un très grand anonymat aux utilisateurs, qui peut être exploité pour dissimuler des crimes; les forces de l'ordre sont souvent incapables de démanteler les activités illégales qui se déroulent sur le Web clandestin, car les acteurs malveillants sont en mesure de s'adapter et déplacer leurs activités rapidement.
- Les cryptomonnaies créent de multiples problèmes à l'application de la loi et à la réglementation en raison de l'évolution des technologies, notamment pour rende le traçage difficile, de l'insuffisance des capacités et de la formation au sein des forces de l'ordre et du système judiciaire dans son ensemble, des obstacles en matière de compétence et de l'incapacité d'adapter certaines lois.
- La mésinformation peut se répandre facilement sur Internet et faciliter la création ou la propagation de contenu préjudiciable. Les individus peuvent s'appuyer sur la mésinformation pour justifier des méfaits ou des crimes ultérieurs, tant en ligne que hors ligne.
- Les entreprises de médias sociaux ont pris certaines mesures d'autorégulation pour modérer le contenu préjudiciable sur leurs platesformes, notamment le retrait de la mésinformation, mais il subsiste des problèmes de transparence, de responsabilité et de cohérence. De plus, certaines méthodes de modération peuvent conduire à la suppression excessive de contenu légal.

Les progrès des TIC ont eu des répercussions spectaculaires sur presque tous les aspects de la vie quotidienne, dont beaucoup étaient imprévues ou inattendues. De nouvelles platesformes et de nouveaux outils numériques sont régulièrement mis sur le marché, souvent sans tenir compte de la manière dont ils peuvent être exploités à des fins préjudiciables. Ce chapitre démontre comment les outils numériques — tels que les instruments financiers (p. ex. les cryptomonnaies ou les sites de sociofinancement), le Web clandestin (*Dark Web*) et les platesformes de médias sociaux — peuvent faciliter le financement, la dissimulation et la diffusion d'actes et de contenus nuisibles cyberfacilités, y compris la mésinformation. Bien que ces outils ne soient pas illégaux, ils sont peu surveillés, largement décentralisés et peuvent être utilisés pour faciliter les

comportements criminels ou autrement dommageables, ce qui rend plus difficiles la détection, la surveillance et la lutte contre les actes préjudiciables. Ils créent en fin de compte des écueils pour lesquels les forces de l'ordre ne constituent pas toujours la meilleure solution, contrairement à une combinaison d'autorégulation de la plateforme, d'éducation à la culture numérique, de redirection du contenu et de blocage du contenu, entre autres.

Ce chapitre commence par décrire les outils financiers employés pour financer et faciliter une variété de comportements criminels et nuisibles. Les sites de sociofinancement et les cryptomonnaies sont eux-mêmes légaux, mais sont apparus comme des moyens de dissimuler le mouvement de grandes quantités d'argent. En général, les lacunes réglementaires et les ressources techniques limitées des forces de l'ordre ont rendu ces outils financiers attrayants pour les auteurs de cybermenaces.

Ensuite, le chapitre examine plusieurs outils courants permettant de renforcer l'anonymat en ligne. Le Web invisible, le Web clandestin et réseaux privés virtuels (RPV) permettent aux utilisateurs de dissimuler certains types de renseignements sur eux-mêmes ou sur les documents qu'ils partagent. Comme les autres outils abordés dans ce chapitre, ils ne sont pas intrinsèquement illégaux et ont des usages positifs et bénéfiques. Pourtant, lorsqu'ils sont utilisés par des auteurs de cybermenaces, ils peuvent masquer des renseignements importants, tels que l'identité et la localisation physique des auteurs. Dans d'autres cas, les utilisateurs bien intentionnés de ces outils peuvent ouvrir des canaux permettant aux auteurs de cybermenaces de perpétrer des méfaits.

Une autre section traite de la mésinformation et des menaces pouvant être dues à sa propagation. Ces dernières années, la mésinformation, y compris la mésinformation visuelle (qui peut être grossière ou simpliste comme très perfectionnée), a pris une place de plus en plus grande dans le discours en ligne et a été rattachée à des croyances complotistes qui ont inspiré des actes préjudiciables et criminels. Le comité d'experts relève que, dans une large mesure, ce genre d'activités nuisibles sont menées à l'aide de services qui accueillent le contenu généré par les utilisateurs, comme les platesformes de médias sociaux.

Le chapitre traite ensuite des platesformes de médias sociaux en général. D'une part, ces platesformes relient des gens du monde entier d'une manière qui rend possible la liberté d'expression et le discours critique; d'autre part, cette connectivité accrue a également permis la création et le partage de contenu criminel, extrémiste et haineux. De même, la mésinformation et le contenu trompeur sont aussi facilement partagés sur les platesformes de médias sociaux. Cette section traite particulièrement des moyens par lesquels ces platesformes

tentent de lutter contre de tels comportements préjudiciables — en grande partie par l'autorégulation, mais aussi avec l'intervention de l'État.

En conclusion de ce chapitre, le comité d'experts montre que la capacité des différents ordres de gouvernement, des forces de l'ordre et des entreprises de médias sociaux à faire appliquer les lois et politiques en vigueur est limitée et à quel point les efforts actuels de modération du contenu sont inefficaces. Il décrit par ailleurs certaines tactiques préventives, notamment l'éducation à la culture numérique et la redirection et le blocage de contenu.

4.1 Outils financiers

4.1.1 Sites de sociofinancement

Le sociofinancement permet « de lever [*sic*] des fonds en recueillant de petites contributions individuelles auprès d'un grand bassin de donateurs par l'entremise de platesformes en ligne » telles que GoFundMe (BDC, 2022). Il est utilisé pour diverses bonnes causes, mais aussi parfois pour financer des activités criminelles ou autrement préjudiciables. Par exemple, le convoi de camions qui a convergé vers Ottawa en janvier 2022 et a procédé à des blocages illégaux a été en partie financé par des dons de sociofinancement provenant du Canada et de l'extérieur (SECU, 2022a). Dans une déclaration au Parlement, GoFundMe — une importante plateforme de sociofinancement utilisée par le convoi — a expliqué que 88 % des fonds recueillis pour le convoi sur sa plateforme provenaient du Canada, 86 % des donateurs semblant être canadiens (SECU, 2022b).

Il y a des lacunes réglementaires et des difficultés de mise en application de la loi en ce qui concerne les sites de sociofinancement

Le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) surveille les transactions concernant les groupes impliqués dans le terrorisme *et al*erte les autorités en cas d'activités financières suspectes (CANAFE, 2021b); toutefois, les activités de nombreux groupes extrémistes passent inaperçues (Thompson, 2022; Tworek, 2022). La collecte de fonds par des groupes extrémistes qui violent les conditions d'utilisation des plateformes de sociofinancement est relativement courante et n'est pas une pratique nouvelle (Tworek, 2022), mais contrairement aux banques et autres institutions financières, les sites de sociofinancement n'étaient pas tenus de signaler les transactions suspectes au CANAFE avant le début de 2022 (GC, 2022a). Barry MacKillop, directeur adjoint de l'unité de renseignement du CANAFE, a expliqué que, bien que les platesformes de sociofinancement basées aux États-Unis n'étaient pas soumises aux lois canadiennes à l'époque du convoi, « les entreprises

de traitement des paiements ayant une présence au Canada et les banques canadiennes par qui transitent les fonds à destination ou en provenance de ces platesformes étaient soumises aux exigences d'enregistrement et de déclaration » (SECU, 2022a).

Le gouvernement fédéral — en vertu des pouvoirs que lui confère la *Loi sur les mesures d'urgence* — a ordonné à toutes les platesformes de sociofinancement en ligne (y compris celles traitant des cryptomonnaies) de déclarer au CANAFE si elles détenaient des fonds appartenant à une personne membre du convoi (FIN, 2022). Bien que ces mesures aient été temporaires, le gouvernement du Canada a annoncé qu'il introduirait un acte législatif visant à rendre plus claires les exigences de déclaration des sociétés de sociofinancement (GC, 2022a). Il a confirmé cette annonce dans son budget 2022, dans le cadre d'efforts plus larges visant à renforcer les outils législatifs et d'application de la loi contre le blanchiment d'argent et le financement du terrorisme (GC, 2022b).

Certains craignent qu'avec ces nouvelles règles, le gouvernement aille trop loin (Durrani *et al.*, 2022) et que l'obligation de déclaration au CANAFE pour les entreprises établies à l'extérieur du Canada soit difficile à appliquer (Karadeglija, 2022). Des questions se posent quant à savoir si le gouvernement peut réellement exercer une telle autorité, étant donné que la nature décentralisée et anonyme des échanges de sociofinancement remet déjà en question l'application de la réglementation existante (Swartz, 2021). Cette situation est aggravée par les capacités restreintes du CANAFE, le fort volume de données reçues et la perception que les répercussions sur les institutions financières qui ne se conforment pas aux exigences de déclaration seront faibles (Carvin *et al.*, 2021a).

4.1.2 Cryptomonnaies

Les monnaies numériques sont des instruments qui permettent le paiement par transactions électroniques (Frankenfield, 2022a). Ces monnaies — qui comprennent les échanges par débit, crédit et virements électroniques effectués par l'entremise des banques traditionnelles, ainsi que les monnaies virtuelles — représentent un écosystème de produits vaste et en rapide évolution, dont seule une partie est réglementée. Certaines d'entre elles sont échangeables contre d'autres monnaies, que ce soit d'autres types de monnaies numériques ou des monnaies émises par une banque centrale, comme le dollar canadien (c.-à-d. une monnaie fiduciaire). Certaines sont liées de manière permanente à une plateforme particulière (p. ex. les monnaies de jeu, qui ne peuvent généralement pas être directement rachetées ou échangées contre d'autres monnaies), tandis que d'autres sont des points de récompense (souvent échangés contre des

marchandises ou des offres de remboursement). D'autres encore, cependant, n'entrent dans aucun système de classification (Frankenfield, 2022a).

Les monnaies virtuelles, qui sont souvent associées aux cryptomonnaies, aux monnaies de jeu et aux points de récompense, sont un sous-ensemble de monnaies numériques qui ne sont pas associées à une banque centrale ou émises par une telle banque. Les cryptomonnaies sont un type de monnaie virtuelle ouverte qui, contrairement à de nombreux genres de points de récompense ou à certaines monnaies d'application, peut être échangée contre d'autres monnaies numériques ou fiduciaires (Frankenfield, 2021). Il s'agit généralement, mais pas toujours, de monnaies décentralisées non contrôlées ou gérées par une institution donnée, ce qui les différencie donc des monnaies émises par les banques centrales (Frankenfield, 2021). Cette section traite des cryptomonnaies décentralisées et ouvertes, en raison de leur popularité croissante dans divers crimes cyberfacilités.

Les cryptomonnaies sont décentralisées et facilitent l'anonymat des utilisateurs

Les cryptomonnaies sont des nouveaux produits financiers introduits en 2008. En 2018, plus de 1 800 types de devises avaient été créés, notamment le bitcoin, l'éther, le monero, le ripple et le litecoin (Kethineni et Cao, 2020). Contrairement aux autres systèmes de paiement (p. ex. l'argent comptant ou le crédit), les cryptomonnaies fonctionnent généralement indépendamment d'une autorité centralisée (p. ex. une banque ou un gouvernement), qui contrôle la légitimité des transactions ou la quantité de monnaie en circulation (ARC, 2021). Le système fonctionne plutôt grâce à des enregistrements de transactions publiques validées (Frankenfield, 2022b). Par exemple, le bitcoin utilise une combinaison de cryptographie et de chaînes de blocs pour suivre et certifier les transactions entre utilisateurs (Berentsen et Schär, 2018). En bref, les transactions sont enregistrées dans des « blocs », qui sont ensuite reliés à un grand livre public des transactions, lequel est vérifié et inaltérable; des processus de chiffrement utilisant un ensemble de « clés » publiques et privées garantissent en outre l'intégrité de chaque transaction (Berentsen et Schär, 2018).

Les cryptomonnaies reposent sur des principes de confidentialité et de sécurité, mais leurs différents types présentent des caractéristiques de confidentialité et de conception variables. Monero, par exemple, propose des *adresses furtives*, qui sont des portefeuilles à usage unique créés lorsqu'un utilisateur lance une transaction (Kanstrén, 2021). D'autres monnaies transmettent les informations relatives aux transactions par le réseau The Onion Route (Tor[8]) ou n'enregistrent pas l'identité

8 Les navigateurs anonymes cryptés tels que Tor ne sont pas utilisés exclusivement sur le Web clandestin. Ils sont conçus pour protéger la vie privée de leurs utilisateurs, et ont donc de multiples applications bénéfiques (Lukings et Lashkari, 2022b).

ou l'emplacement de l'expéditeur. Le degré de confidentialité des cryptomonnaies dépend également des pratiques individuelles des utilisateurs, et peut être accru au moyen de tactiques telles que le changement fréquent de pseudonyme ou l'utilisation de services de masquage IP (Baron *et al.*, 2015). La possibilité d'anonymat, la capacité d'échapper à l'impôt, l'absence d'autorité centralisée et la croissance des marchés cachés en ligne ont fait des cryptomonnaies des modes de paiement attrayants pour les biens ou services illégaux; plusieurs des plus grands marchés cachés de ces dix dernières années (p. ex. Silk Road, AlphaBay, Hansa) acceptaient au moins un type de cryptomonnaie avant d'être fermés (Kethineni et Cao, 2020). Fait notable, après s'être vu refuser le service par les principaux émetteurs de cartes de crédit comme Visa, Mastercard et Discover pour sa modération insatisfaisante du matériel d'abus pédosexuel (MAP), Pornhub a changé de cap pour n'accepter que les cryptomonnaies (Goodwin, 2020) (chapitre 3).

Les cryptomonnaies peuvent servir à blanchir de l'argent et à financer des crimes

Le marché des cryptomonnaies prend de l'expansion, tout comme le nombre de plateformes d'échanges de cryptomonnaies. De nombreux utilisateurs choisissent d'effectuer des transactions dans des plateformes d'échange décentralisées (DEX) en partie en raison de leurs frais de transaction moins élevés, mais aussi parce qu'il est plus facile d'y fonctionner de manière anonyme (Clark *et al.*, 2022; Khan et Ali Hakami, 2022). Sur le plan de la sécurité publique, les cryptomonnaies soulèvent plusieurs préoccupations, comme la possibilité de les utiliser pour le blanchiment d'argent, le paiement de rançons et le financement du terrorisme et autres crimes financiers, parce qu'elles sont difficiles à suivre (Kethineni et Cao, 2020; Davis, 2021) (encadré 4.1). Il a notamment été avancé que la facilité des transferts de cryptomonnaies associée à la difficulté de les retracer a joué un rôle clé dans l'essor des opérations par rançongiciels de grande envergure (Weaver, 2021). Selon le Centre canadien pour la cybersécurité (2022a), bien que « les services policiers connaissent un certain succès lorsque vient le temps de retracer, et dans certains cas, de récupérer des sommes volées, les auteurs de cybermenace continuent de perfectionner et de développer des techniques pour masquer des transactions financières illicites » et « le blanchiment d'argent au moyen de cryptomonnaie continuera à faciliter la montée de la cybercriminalité ».

Encadré 4.1 Collecte de fonds en ligne pour des activités terroristes

Les espaces numériques peuvent servir « à inspirer, à encourager, à organiser, à financer et à planifier des gestes de violence » (CCECPV, 2018). Les organisations terroristes telles qu'Al-Qaïda, par exemple, partagent en ligne des instructions sur la manière de perpétrer des actes violents, notamment sur l'utilisation des armes. Les outils technologiques financiers (cryptomonnaies comprises) ont joué un rôle important dans le financement du terrorisme ces dernières années (Davis, 2021). Il n'est pas difficile de mettre en place des campagnes de collecte de fonds de grande envergure sur les médias sociaux pour solliciter des dons qui, une fois reçus, pourront être facilement transférés dans le monde entier grâce aux platesformes et aux échanges de cryptomonnaies. Même si les platesformes de médias sociaux interdisent les campagnes de collecte de fonds pour des activités terroristes, il est possible aux collecteurs de fonds de communiquer individuellement avec les donateurs potentiels au moyen d'une messagerie chiffrée, ce qui peut rendre difficile le suivi, la surveillance ou l'interdiction de ces campagnes (Weimann, 2016; Davis, 2021). Ces activités peuvent être encore plus compliquées à retracer si elles migrent vers le Web clandestin, un mouvement encore facilité par la coordination entre les organisations terroristes (Weimann, 2016).

Le CANAFE a été fondé en 2000 pour répondre aux normes internationales de lutte contre le blanchiment d'argent, et a été élargi pour aider à déceler les stratagèmes de financement du terrorisme en 2001 (Carvin *et al.*, 2021a). Il recueille, analyse et stocke des renseignements financiers provenant de milliers de sources, notamment de comptables, de sociétés de services bancaires et financiers, de casinos et de compagnies d'assurance. Lorsqu'il existe des motifs raisonnables de soupçonner une activité illégale, les renseignements peuvent être communiqués aux forces policières ou aux organismes de sécurité appropriés (CANAFE, 2021a). Le CANAFE exige la collaboration des intermédiaires — ceux qui facilitent le transfert et l'échange de valeurs — pour déclarer les transferts financiers importants ou suspects. Il s'appuie également sur l'autodéclaration des institutions financières (CANAFE, 2022), ce qui complique les efforts d'application de la loi étant donné l'anonymat des cryptomonnaies et des échanges qui leur sont associés. En 2019, la réglementation relative au CANAFE a été modifiée pour tenir compte des monnaies virtuelles (y compris les cryptomonnaies). En vertu de cette modification, par exemple, les négociants de cryptomonnaies qui servent des

clients canadiens sont traités comme des entreprises de services monétaires, lesquelles sont soumises aux exigences de déclaration du CANAFE (GC, 2019b; Carvin *et al.*, 2021a) (chapitre 5).

La réglementation des cryptomonnaies est difficile à appliquer

Les cryptomonnaies peuvent partager de nombreuses qualités avec les monnaies traditionnelles et, dans certains cas, sont échangées comme des titres ou des produits d'investissement. Au Canada, les valeurs mobilières et les placements sont réglementés par des exigences d'enregistrement pour les courtiers, les conseillers et les gestionnaires de fonds, par des exigences propres aux bourses et aux marchés et par des exigences de déclaration et de communication (d'Anglejan-Chatillon *et al.*, 2021). Avec les cryptomonnaies, on ne sait pas toujours qui tenir responsable des opérations illégales, et encore moins comment. Les DEX, en particulier, sont souvent peu surveillées et les transactions ne sont pas effectuées par des intermédiaires centraux de confiance; toutes les transactions sont essentiellement effectuées de personne à personne (Chainlink, 2022). Cela soulève plusieurs questions en matière d'application de la loi, comme celle de savoir quels gouvernements devraient être responsables de la surveillance du statut juridique d'une DEX et qui est considéré comme partie prenante d'une DEX et donc responsable du respect de la réglementation par cette bourse (GC, 2021c). Les Autorités canadiennes en valeurs mobilières (ACVM) ont publié des lignes directrices sur la négociation des cryptomonnaies et sur la réglementation applicable aux platesformes de négociation de cryptoactifs (ACVM, 2020; ACVM et OCRCVM, 2021). La réglementation des valeurs mobilières relève de la compétence des provinces et des territoires et est relativement uniforme dans tout le pays. Cependant, les produits dérivés reposant sur les monnaies virtuelles sont réglementés à la fois par les gouvernements provinciaux et territoriaux et par le fédéral (d'Anglejan-Chatillon *et al.*, 2021).

Les plateformes d'échanges de cryptomonnaies ne sont pas toutes prêtes à se conformer à la réglementation, et certaines bourses étrangères pourraient décider de quitter le marché canadien (Sobowale, 2021). Fait notable, les ACVM ont annoncé en août 2022 que leurs membres (les organismes de réglementation des valeurs mobilières de chaque province et territoire) s'attendent désormais à ce que les platesformes d'échange de cryptomonnaies s'inscrivent auprès de leur principal organisme de réglementation et, dans l'intervalle, acceptent de se conformer à des conditions qui répondent aux préoccupations en matière de protection des investisseurs (CSJO, 2022). Elles ont également annoncé que leurs membres peuvent prendre des mesures si une plateforme de négociation n'est pas prête à se conformer à cette attente. De l'avis du comité d'experts, il est parfois difficile de savoir quelle est la réglementation qui s'applique le mieux aux

cryptomonnaies, ou s'il faut appliquer une réglementation stricte si cela amène les négociants en cryptomonnaies à quitter le marché canadien.

À l'étranger, il existe diverses pratiques réglementaires concernant les cryptomonnaies. Le modèle financier australien considère les monnaies virtuelles comme des biens (ce qui est également vrai au Canada lorsque les cryptomonnaies ne sont pas négociées sous forme de valeurs mobilières) et permet les échanges à condition qu'ils soient enregistrés auprès de l'Australian Transaction Reports and Analysis Centre (Centre australien de déclaration et d'analyse des transactions) (AUSTRAC, 2018; Smith, 2021a). Cependant, tous les pays n'ont pas adopté un tel procédé. Aux États-Unis (comme au Canada), les monnaies virtuelles peuvent être considérées comme des valeurs mobilières, des marchandises, des devises ou des biens, selon que l'utilisateur traite avec la Securities and Exchange Commission, la Commodity Futures Trading Commission, le département du Trésor ou l'Internal Revenue Service (Smith, 2021b). Au Royaume-Uni, la plupart des échanges de cryptomonnaies doivent être enregistrés auprès de la Financial Conduct Authority (FCA) (Hammond et Ehret, 2021). En outre, la FCA a élaboré des règlements en matière de diligence raisonnable à l'égard des clients (surnommées « *know your customer* », en anglais) et de lutte contre le blanchiment d'argent, ainsi que des règlements destinés à combattre le financement du terrorisme. Les cryptomonnaies n'ayant pas cours légal au Royaume-Uni, elles sont taxées en fonction des gains et des pertes découlant de leur utilisation, qui est limitée par l'interdiction de négocier des dérivés de cryptomonnaies. Au sein de l'Union européenne, les lois et règlements fiscaux varient considérablement d'un État à l'autre (Hammond et Ehret, 2021).

Certaines plateformes d'échanges de cryptomonnaies, dans le but de compléter ou de devancer la réglementation gouvernementale, optent même pour l'autorégulation. Le 7 février 2022, un groupe de 16 bourses du monde entier, réunies par la société de logiciels de surveillance des risques Solidus Labs, a annoncé le lancement de la Crypto Market Integrity Coalition (Coalition pour l'intégrité des marchés de cryptomonnaies) (Lang, 2022). La coalition a pour objectif déclaré d'« accroître l'intégrité et l'efficacité du fonctionnement des marchés d'actifs numériques » [traduction libre] (CMIC, 2022). Elle vise à maintenir l'intégrité et l'efficacité des marchés indépendamment des exigences réglementaires et prévoit de le faire en surveillant, détectant et éliminant régulièrement les pratiques de marché déloyales (CMIC, 2022). En décembre 2022, la coalition cherchait à faire signer à d'autres platesformes d'échange de cryptomonnaies un « engagement public et sans équivoque », mais n'a pas précisé d'autres projets.

Malgré les efforts déployés pour réglementer l'espace des cryptomonnaies et appliquer la réglementation actuelle, il est difficile pour les forces de l'ordre de faire respecter l'*utilisation* légale des cryptomonnaies.

De nombreuses cryptomonnaies couramment utilisées sont théoriquement traçables par les experts et les organismes gouvernementaux, mais le faible nombre de ces experts, le coût élevé et l'infrastructure nécessaire pour suivre les transactions et appliquer les règlements ont incité la Gendarmerie royale du Canada (GRC) à étendre son programme de cryptomonnaies en formant davantage d'agents pour aider durant les enquêtes (Northcott, 2022). Dans le même temps, on a aussi assisté à des avancées réduisant la traçabilité, notamment au moyen de DEX et de monnaies à confidentialité renforcée, par la création de parcours de transaction alambiqués grâce à la conversion des fonds illicites en différentes cryptomonnaies ou par l'utilisation de services de *mixage* qui, essentiellement, brouillent le chemin des transactions pour des frais minimes (Clark *et al.*, 2022; Europol, 2022; Freeman Law, 2022). Selon l'expérience des membres du comité d'experts, dans certains cas, ces techniques évoluées, augmentent la difficulté de retracer les transactions en cryptomonnaies à un niveau qui dépasse la capacité ou l'aptitude de la grande majorité des forces de l'ordre.

Les utilisateurs de cryptomonnaies peuvent être la cible de vols et de fraudes

Entre octobre 2020 et mai 2021, la Federal Trade Commission des États-Unis a signalé plus de 80 millions de dollars US de pertes dues à des escroqueries à l'investissement en cryptomonnaies (Fletcher, 2021). Les tactiques classiques d'hameçonnage, de fraude et d'extorsion consistent à inciter les victimes à transférer des cryptomonnaies à des acteurs malveillants; les actifs transférés n'étant souvent pas assurés par un intermédiaire ou un organisme de contrôle (comme pourrait l'être une monnaie en ligne traditionnelle), les victimes ont peu d'options pour les récupérer après le vol (GC, 2021d; AARP, 2022). Les plateformes d'échanges de cryptomonnaies peuvent également être victimes de vol ou de faillite (Lane, 2022). Souvent, lorsque les utilisateurs achètent des cryptomonnaies par l'intermédiaire d'une bourse, leurs actifs sont conservés dans des portefeuilles propres à la bourse, dont les clés privées ne sont connues que de cette bourse. Si un auteur de cybermenaces compromet la sécurité d'une bourse, il peut obtenir les renseignements nécessaires pour prendre le contrôle des portefeuilles activement connectés au réseau de cette bourse et donc des actifs de ses clients. Dans ce cas, ou en cas de défaillance pour des raisons commerciales, les utilisateurs ont peu de recours pour récupérer leurs actifs volés ou perdus (p. ex. AscendEx, BitMart et Liquid) (Lane, 2022).

Un marché de valeurs mobilières de type boursier reposant sur la valeur des monnaies virtuelles a également émergé, obligeant les gouvernements du monde entier à se pencher sur la façon de réglementer ce nouveau genre d'échange d'actifs (ARC, 2021). Comme pour les investissements dans d'autres marchés

volatils, la valeur d'une monnaie virtuelle échangée peut varier considérablement. En outre, des stratagèmes ont été utilisés pour influer sur la valeur des cryptomonnaies afin d'obtenir un avantage sur les autres négociateurs. Selon un rapport de Bitwise, jusqu'à 95 % du volume d'échange de bitcoins déclaré est faux ou représente des échanges non économiques, qui cherchent à faire croire que l'actif est très liquide (un stratagème connu sous le nom d'« opérations fictives ») (Bitwise Asset Management, 2019); le pourcentage exact varie selon les études, mais toutes constatent également que la majeure partie du volume d'échange de bitcoins déclaré est associé à des opérations fictives (Le Pennec *et al.*, 2021). Comme généralement ces échanges ne sont pas réglementés et sont décentralisés, déterminer si une source de fixation du prix ou de données d'échange est fiable n'est pas une tâche simple et constitue un domaine actif de la recherche en analyse financière (Vidal-Tomás, 2022).

4.2 Outils d'anonymat en ligne

4.2.1 Web invisible et Web clandestin

Le Web clandestin est une partie du Web invisible

Les moteurs de recherche comme Google ne font qu'effleurer le contenu d'Internet (figure 4.1). Le *Web invisible* désigne toute partie d'Internet non indexée (c.-à-d. non cataloguée par les moteurs de recherche traditionnels), et qui peut réclamer pour y accéder un mot de passe, le chiffrement ou un logiciel spécialisé (Weimann, 2016; Sheils, 2021). Parmi les exemples de contenu du Web invisible, on peut citer des services bancaires en ligne, des comptes de courriel personnels, des bases de données d'utilisateurs et des sites réservés aux membres (Lukings et Lashkari, 2022b). Le *Web clandestin* est un sous-ensemble du Web invisible, et on ne peut y accéder qu'en utilisant des navigateurs spécialisés comme Tor (Weimann, 2016; Chertoff, 2017; Lukings et Lashkari, 2022b). Le degré d'anonymat des utilisateurs est plus élevé sur le Web clandestin que sur l'Internet indexé (c.-à-d. le Web ouvert) ou que sur le Web invisible. L'utilisation de services comme Tor permet généralement de se protéger de la surveillance et de l'identification par de potentiels observateurs grâce à de multiples couches de chiffrement (Hatta, 2020).

L'anonymat et la confidentialité sur le Web invisible en ont fait un outil précieux pour les défenseurs de la société civile tels que les journalistes, les militants et les lanceurs d'alerte, qui travaillent parfois dans un environnement hostile; cependant, il crée également un milieu attractif pour les activités criminelles — surtout le Web clandestin, qui peut dissimuler des auteurs de cybermenaces (Kalpakis *et al.*, 2016; Lukings et Lashkari, 2022b). Par exemple, l'un des usages courants du Web clandestin est l'accès aux *marchés cachés*, qui sont des

platesformes de vente et d'achat de biens et services illégaux, tels que le MAP, les drogues illicites, les produits de contrefaçon ou les armes (Lukings et Lashkari, 2022b). Une autre utilisation fréquente consiste à partager anonymement des liens vers du MAP (qui n'est lui-même pas hébergé sur le Web clandestin, mais plutôt sur le Web ouvert ou sur le Web invisible) (CCPE, 2021). L'anonymat fait également en sorte qu'il est difficile ou presque impossible de faire appliquer la réglementation sur le Web invisible et le Web clandestin.

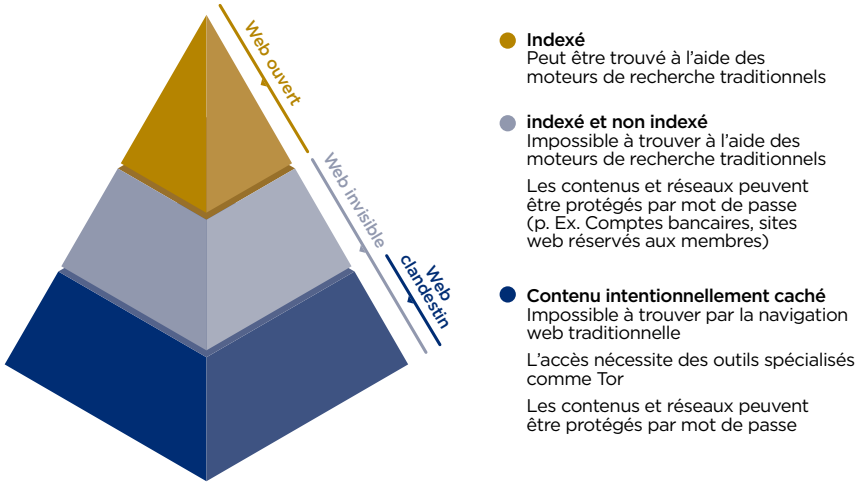


Figure 4.1 Les couches d'Internet

Internet peut être divisé en trois parties : le Web ouvert, qui est accessible par les navigateurs Web traditionnels et indexé par les moteurs de recherche, le Web invisible, qui est souvent protégé par mot de passe, et le Web clandestin, qui est intentionnellement caché. Le Web clandestin est un sous-ensemble du Web invisible.

Il est difficile de déterminer le volume et les catégories de contenu présent sur le Web clandestin. À la fin du mois d'août 2022, on comptait environ 2,8 millions d'utilisateurs actifs de Tor dans le monde (Projet Tor, 2022), mais ce chiffre n'est pas révélateur de la façon dont les individus utilisent le service. Diverses études ont analysé des sections de contenu sur le Web clandestin, mais il est difficile d'en effectuer des analyses détaillées en raison de sa taille et de sa nature dynamique (Monk *et al.*, 2018). Grâce au fort anonymat sur le Web clandestin, les cybercrimes sont plus difficiles à prévenir, à détecter et à contrer (Kalpakis *et al.*, 2016; Lukings et Lashkari, 2022b). Les difficultés sont accrues par les complexes questions de compétences dues à l'emplacement de l'utilisateur, du serveur et du crime, ce qui

entrave souvent les enquêtes des forces de l'ordre sur ces espaces numériques (Lukings et Lashkari, 2022b).

Les marchés cachés reposent couramment sur les cryptomonnaies (Patil, 2019), dont l'anonymat et la confidentialité en ont fait des modes de paiement populaires pour de nombreux acteurs malveillants, y compris certaines organisations terroristes; cela a incité des experts à s'inquiéter du fait que les monnaies virtuelles puissent devenir des « monnaies criminelles » (Kethineni et Cao, 2020). De multiples enquêtes ont provoqué la fermeture de marchés cachés hébergés ou exploités par des criminels situés au Canada, qui étaient impliqués dans la vente de drogues illégales sur le Web clandestin (Patil, 2019; GRC, 2020b). AlphaBay, un des plus gros marchés cachés jusqu'à sa fermeture après une opération mondiale en 2017, a été créé et géré par un citoyen canadien (FBI, 2017). Cependant, les opérations policières spéciales visant les marchés cachés ne sont pas parvenues à diminuer à long terme le nombre de trafiquants de drogues illicites, qui peuvent rapidement adapter leurs tactiques et vendre leurs produits ailleurs (Décary-Hétu et Giommoni, 2017).

4.2.2 Réseaux privés virtuels (RPV)

Les RPV sont des outils utiles lorsqu'ils sont utilisés de manière appropriée, mais ils peuvent également exposer les utilisateurs à différentes menaces à leur sécurité

Ces dernières années, l'utilisation de RPV par les particuliers et les entreprises a augmenté (Vigderman et Turner, 2022). Proposant plusieurs protocoles (qui présentent tous un éventail de propriétés de confidentialité et de sécurité), un RPV permet à un utilisateur d'établir une connexion Internet virtuelle point à point vers un réseau ou une adresse IP distant. Par exemple, un utilisateur de Montréal peut faire croire qu'il se trouve à Glasgow avec son appareil. Cependant, tous les RPV n'offrent pas les mêmes fonctions de confidentialité, de sécurité ou de chiffrement; dans certains cas, l'utilisation d'un tel instrument peut mettre en danger la confidentialité et la sécurité de l'utilisateur (Dinha, 2021).

Bien qu'ils partagent la même appellation, les RPV utilisés par les entreprises ont des objectifs différents et présentent des risques différents de ceux des RPV que les particuliers peuvent employer pour se connecter à Internet (Dinha, 2021). Les RPV d'entreprise servent généralement à connecter en toute sécurité un utilisateur distant au réseau interne de l'organisation, ce qui est utile pour les personnes qui travaillent à distance et qui doivent accéder à des données d'entreprise sécurisées par des réseaux non fiables. La sécurité de ce type de RPV dépend de la mise à jour régulière du système pour le protéger contre les entités malveillantes qui le ciblent (Palmer, 2021).

Les RPV grand public connectent les individus à Internet et peuvent servir différents buts. D'après une source, éviter le vol d'identité et protéger les données personnelles sont deux des utilisations les plus courantes des RPV grand public, tandis que d'autres utilisateurs peuvent souhaiter contourner les restrictions de contenu imposées par leur communauté en masquant leur propre adresse IP (p. ex. pour accéder au catalogue Netflix ou au service de diffusion publique d'un autre pays) (Vigderman et Turner, 2022). Les RPV peuvent faciliter ces objectifs, mais ils peuvent aussi exposer les utilisateurs à de nouveaux risques (Dinha, 2021). De nombreux services de RPV sont proposés sur Internet sous forme gratuite ou payante, mais rien ne garantit qu'ils procurent la confidentialité, la sécurité et l'anonymat promis, ni que le fournisseur lui-même ne suivra pas ou ne compromettra pas les données ou la sécurité de l'utilisateur. Il est donc important pour les utilisateurs potentiels de RPV de comprendre comment ces outils fonctionnent et qui les exploite, et les gens devraient utiliser uniquement les RPV de fournisseurs de confiance.

4.3 Mésinformation

4.3.1 Diffusion en ligne de la mésinformation

Diffuser de la mésinformation n'est pas illégal, mais cela peut causer des préjudices

La mésinformation est définie de manière générale comme de l'information fausse ou trompeuse (Heer *et al.*, 2021). La *désinformation*, quant à elle, est un « effort coordonné ou délibéré pour faire circuler sciemment des informations erronées afin d'acquérir de l'argent, le pouvoir ou une réputation » [traduction libre] (Swire-Thompson et Lazer, 2020). Un concept apparenté est la *malinformation*, qui est une information réelle utilisée pour induire en erreur (souvent par exagération) et causer des préjudices (UNESCO, 2018; Centre canadien pour la cybersécurité, 2022b). Dans ce rapport, le comité d'experts utilise le terme de *mésinformation* pour décrire ces trois concepts parce qu'il peut être difficile de déterminer l'intention et parce que la distinction, en fin de compte, n'influe pas sur les conséquences potentielles.

Si la diffusion de la mésinformation en ligne ne constitue pas en soi un acte criminel et ne relève généralement pas du mandat actuel des forces de l'ordre[9], elle peut entraîner des préjudices importants et soutenir ou encourager la criminalité (Europol, 2020a); plusieurs menaces et préjudices qui peuvent en résulter sont étudiés à la section 4.4. Comme nous le démontrons dans la présente

9 Le Service canadien du renseignement de sécurité (SCRS) a pour mandat de détecter les campagnes de désinformation, souvent menées par des acteurs étrangers, qui ont des répercussions sur la sécurité nationale, notamment en influençant les processus démocratiques canadiens, et d'enquêter dessus (SCRS, 2021a).

section, la désinformation peut contribuer à motiver des actes haineux et violents, et elle peut être difficile à contenir. Cette section se concentre particulièrement sur les TIC et sur les plateformes qui reposent sur le contenu produit par les utilisateurs, ce qui fait en sorte que la désinformation est un problème complexe, tentaculaire et sans cause idéologique ou méthode de transmission unique. La lutte contre la désinformation en ligne nécessite une démarche globale, qui dépasse le seul contenu (Tworek, 2020).

Les TIC peuvent faciliter la diffusion de la désinformation

Historiquement, la désinformation s'est répandue par le biais de différents forums et médias pour des raisons politiques et économiques; elle a longtemps été utilisée comme un outil de guerre, pour influencer les résultats économiques et pour éroder la confiance dans les institutions (Rid, 2020). Les TIC peuvent faciliter la diffusion rapide d'informations à une échelle encore plus grande que ce que permettaient auparavant les canaux de distribution de la presse écrite, de la radio ou de la télévision, ce qui rend la désinformation plus difficile à contrôler qu'autrefois (Rid, 2020). En outre, compte tenu de sa rapidité et de la distance qu'elle peut couvrir, la désinformation contemporaine peut se répandre rapidement, sur une grande échelle et sur de plus vastes étendues géographiques. Une analyse de Shao *et al.* (2018) portant sur 14 millions de messages Twitter a révélé que les bots sociaux — des profils contrôlés par logiciel sur les médias sociaux, qui peuvent servir à communiquer des informations utiles — jouent également un rôle disproportionné dans la diffusion de la désinformation, surtout dans les premiers temps, avant que le contenu ne devienne viral. Les données probantes indiquent que les fausses informations en ligne se propagent plus rapidement et plus largement que les informations véridiques, et que la désinformation politique se propage plus rapidement que les autres types de désinformation (Vosoughi *et al.*, 2018).

Comme ailleurs dans le monde, la société canadienne est polarisée (Owen *et al.*, 2019). Des données probantes récentes montrent toutefois que les TIC ne sont pas intrinsèquement une cause de polarisation. La polarisation en ligne peut être due à des événements externes (hors ligne) — comme le déclin de la légitimité perçue des institutions gouvernementales — qui ne sont pas liés à l'activité se déroulant sur les plateformes Web (Benkler *et al.*, 2018; Owen *et al.*, 2019; Bennett et Livingston, 2020; Waller et Anderson, 2021). Dans le même temps, la désinformation qui circule en ligne a un impact sur les croyances des gens. Par exemple, une enquête menée auprès de 1 000 personnes au Québec a révélé que plus de 20 % d'entre elles croyaient ou étaient d'accord avec les théories du complot objectivement fausses ou avec la désinformation circulant sur Internet (Langlois et Sauvageau, 2021).

La même étude a également révélé que les jeunes étaient significativement plus susceptibles de croire ces fausses idées.

La conception de nombreuses platesformes de médias sociaux peut contribuer à amplifier des formes particulières de contenu. Le Centre canadien pour la cybersécurité (2022a) affirme que les algorithmes des médias sociaux ont presque certainement contribué à la propagation de la mésinformation. Par exemple, pour susciter davantage de réactions chez les utilisateurs, l'algorithme de Facebook favorise (et amplifie) systématiquement le contenu émotionnel ou provocateur, qui est plus susceptible de renfermer de la mésinformation (Merrill et Oremus, 2021).

Les platesformes Web contemporaines ont largement supplanté les sources médiatiques traditionnelles, qui comportent généralement une certaine forme de contrôle rédactionnel pour évaluer la véracité des informations et déterminer ce qui doit être communiqué (Trudel, 2021). Les platesformes en ligne ont relégué les fonctions rédactionnelles au second rang, au profit de fonctions automatisées destinées à susciter des réactions émotionnelles à l'information.

La mésinformation peut causer des préjudices directs et indirects, notamment en incitant à la haine et en facilitant la fraude

Au Canada, la prolifération de la mésinformation en ligne a favorisé une hausse de la discrimination, de la marginalisation et de la haine (Tenove *et al.*, 2018; Heer *et al.*, 2021). Par exemple, des informations fausses ou trompeuses sur les médias sociaux reliant la communauté musulmane aux épidémies de COVID-19 ont contribué à l'islamophobie (Al-Qazzaz, 2020). De même, les incidents signalés de racisme anti-asiatique (y compris en ligne) ont augmenté en 2020 et 2021 (Macguire, 2020; Kong *et al.*, 2021), ce qui peut être dû à la mésinformation sur les platesformes de médias sociaux concernant les origines et la propagation de la maladie (section 3.2.2). La mésinformation est également associée à la discrimination et aux préjugés. Des expériences ont montré que l'exposition aux théories du complot concernant les Juifs et les immigrés au Royaume-Uni exacerbait les préjugés envers ces groupes (Jolley *et al.*, 2020). La mésinformation visant à discréditer ou à dénigrer certaines communautés ou identités peut circuler sur le Web (Tenove et Tworek, 2019); comme nous l'avons vu à la section 3.2.2, des groupes aux idéologies haineuses utilisent les TIC pour diffuser leurs messages et trouver des partisans (Tenove *et al.*, 2018).

Dans certains cas, la mésinformation peut être utilisée pour soutenir ou motiver les crimes cyberfacilités. La pandémie de COVID-19, par exemple, a donné l'occasion aux auteurs de cybermenaces d'exploiter la vulnérabilité accrue des utilisateurs à leur profit (OCDE, 2020b). La diffusion de la mésinformation sur de

prétendus remèdes contre la COVID-19 a servi à vendre des produits non réglementés et potentiellement dangereux en ligne, y compris sur le Web clandestin (Europol, 2020a; OCDE, 2020a). La mésinformation favorise également la cybercriminalité en rendant les attaques d'hameçonnage plus efficaces et en facilitant de plus en plus les menaces hybrides (qui « combinent des activités conventionnelles et non conventionnelles, militaires et non militaires [...] pour atteindre des objectifs politiques » [traduction libre]) (Europol, 2020b).

La mésinformation peut nuire aux processus démocratiques et à la liberté d'expression

La *Loi sur la modernisation des élections* du Canada s'attaque à la mésinformation et à l'ingérence étrangère dans les élections en interdisant aux entités et aux individus étrangers d'acheter des publicités pendant une période électorale et en obligeant les platesformes en ligne à publier un registre des publicités partisanes produites pendant une élection (GC, 2018a). Le SCRS a toutefois prévenu que les Canadiens sont souvent la cible de campagnes de mésinformation sur Internet menées par divers auteurs de cybermenaces, notamment commandités par des États étrangers, ce qui a des répercussions sur la sécurité nationale (SCRS, 2018, 2021b). Ces campagnes sur les médias sociaux, menées notamment par des brigades Web, visent souvent à intensifier la polarisation et à miner la confiance dans les différents ordres de gouvernement, dans les institutions et dans le processus démocratique (SCRS, 2021b). Par exemple, un rapport sur la diffusion de la mésinformation pendant les élections fédérales canadiennes de 2021 a relevé que différents groupes qui se méfient de plus en plus des experts gouvernementaux et des médias grand public ont commencé à se réunir, formant une communauté de mésinformation de type « grande tente », qui expose davantage ses membres aux nouvelles et aux idées en général fortement motivées par l'idéologie (Bridgman *et al.*, 2022). Dans le même temps, les recherches indiquent que les fausses rumeurs (c.-à-d. la mésinformation) sont plus susceptibles d'émerger et de réémerger plusieurs fois sur Twitter que les vraies rumeurs (c.-à-d. les faits) (Shin *et al.*, 2018). De même, l'infusion d'un grand volume de mésinformation peut enlever aux gens tout pouvoir d'action en nuisant à leur capacité à rechercher, à recevoir et à partager des informations véridiques et à se forger une opinion et des croyances de façon autonome (Khan, 2021).

4.3.2 Croyances complotistes

Les théories du complot sont une catégorie de mésinformation et sont souvent motivées par des raisons politiques. Ces théories cherchent souvent à « expliquer les événements ou les pratiques comme étant le fait d'acteurs qui abusent secrètement de leur pouvoir pour réaliser leurs [propres] objectifs » [traduction

libre] (Craft *et al.*, 2017) et elles peuvent émerger en réponse à un ensemble de facteurs sociaux et économiques, notamment la méfiance envers les institutions, le ressentiment à l'égard des élites ancré dans la montée des inégalités et le racisme (Tworek, 2020).

Les médias sociaux favorisent les idées complotistes

L'importance des platesformes de médias sociaux dans la propagation des théories du complot est d'autant plus grande qu'elles sont souvent utilisées comme source d'information. Par exemple, au Canada, 24 % des personnes déclarent utiliser Facebook et 24 % déclarent utiliser YouTube comme source d'information (Andrey *et al.*, 2021b). Les utilisateurs canadiens de médias sociaux montrent également un intérêt pour le discours politique; une enquête a révélé que 33 % des personnes au Canada utilisent les platesformes de médias sociaux au moins une fois par semaine pour partager des nouvelles ou des messages politiques, tandis que 30 % commentent les nouvelles ou les messages politiques selon une fréquence similaire (Andrey *et al.*, 2021b).

L'utilisation des médias sociaux comme sources d'information est positivement corrélée avec les croyances dans les théories du complot et la mésinformation (Enders *et al.*, 2021), même quand d'autres facteurs, comme le recours aux médias d'information, la partisanerie, l'âge et l'éducation, sont contrôlés (Stecula et Pickup, 2021). Les utilisateurs des médias sociaux qui accèdent à du contenu plus polarisé sont plus susceptibles de répandre de la mésinformation (Bessi *et al.*, 2016). Cependant, toutes les platesformes n'ont pas le même effet : dans des études américaines publiées en 2021, les individus recourant à Facebook ou YouTube pour obtenir des nouvelles étaient plus susceptibles d'adopter des croyances complotistes que ceux qui utilisaient principalement Twitter (Stecula et Pickup, 2021; Theocharis *et al.*, 2021).

Les croyances complotistes peuvent motiver des actes criminels, y compris la violence

Des études ont constaté des corrélations positives entre la croyance dans les théories du complot et les comportements et intentions criminels (Uscinski et Parent, 2014; Jolley *et al.*, 2019; Rottweiler et Gill, 2020). Des données expérimentales indiquent que le fait d'être exposé à du matériel complotiste joue un rôle dans la hausse des intentions de commettre des crimes communs (p. ex. brûler des feux rouges, utiliser de l'argent liquide pour éviter de payer des impôts) à l'avenir (Jolley *et al.*, 2019). En outre, les personnes ayant des prédispositions complotistes particulièrement fortes sont plus enclines à des actions violentes (Uscinski et Parent, 2014; Rottweiler et Gill, 2020). Comme le montrent les sections suivantes de ce chapitre, les gens peuvent s'appuyer sur la

mésinformation — qui facilite la radicalisation et l'extrémisme — pour justifier la violence hors ligne et d'autres méfaits (y compris le vandalisme), ce qui peut mener à des troubles sociaux. Comme pour d'autres formes de harcèlement et de méfaits en ligne, certaines professions en contact avec le public peuvent être ciblées plus que d'autres (section 3.1.2).

Le lien entre les théories du complot et le comportement criminel a été observé dans le contexte de la pandémie de COVID-19. Par exemple, les fausses affirmations selon lesquelles les ondes radio émises par les tours 5G rendent les gens plus vulnérables à cette maladie ont contribué à la colère contre les gouvernements et même à des réactions violentes (Devlin, 2020; Jolley et Paterson, 2020). Dans le contexte canadien, Global News a obtenu en 2020 un rapport confidentiel du SCRS mettant en garde contre les théories du complot qui associent COVID-19 et technologie 5G, exprimant la crainte que des « extrémistes violents motivés par l'idéologie » [traduction libre] puissent déclencher des incendies criminels et commettre des actes de vandalisme contre l'infrastructure 5G (Bell, 2020). La police a enquêté sur le rôle potentiel des théories du complot à la suite de l'arrestation au Québec de deux personnes pour avoir mis le feu à plusieurs tours cellulaires, dont aucune n'accueillait de l'équipement 5G (Bellemare *et al.*, 2020). Des attaques similaires se sont produites ailleurs dans le monde (Cerulus, 2020; OCDE, 2020b), qui ont pu nuire à la fonctionnalité des systèmes des services d'urgence (Devlin, 2020).

Les croyances ancrées dans les théories du complot sont au cœur de certains mouvements extrémistes violents

Les théories du complot et l'extrémisme violent sont de plus en plus imbriqués (SECU, 2022a). QAnon, l'un des exemples les mieux documentés de mésinformation politique motivant la violence (Winter, 2019; Garry *et al.*, 2021), est un ensemble de théories du complot prétendant à tort qu'« un groupe d'élites adoratrices de Satan et dirigeant un réseau sexuel d'enfants » [traduction libre] tente de contrôler la politique et les médias américains (Ipsos et NPR, 2020). Le mouvement est né et a proliféré sur Internet, et les médias sociaux ont facilité la diffusion de la mésinformation qui lui est rattachée (Garry *et al.*, 2021; Roose, 2021; Lin *et al.*, 2022). Ses membres sont très actifs en ligne; sur Twitter, par exemple, les mots-clics et les phrases liés à QAnon ont été utilisés plus de 20 millions de fois entre janvier et septembre 2020 (BBC News, 2021). Certains de ses adeptes sont passés à l'action hors ligne, participant notamment à l'attaque violente et meurtrière du Capitole en janvier 2021 (Garry *et al.*, 2021; Roose, 2021), qui avait été principalement planifiée en ligne (Frenkel, 2021). On a signalé que d'autres partisans de QAnon ont été accusés de crimes violents, y compris d'enlèvements et de complots d'assassinat (Roose, 2021).

Bien que certains réseaux sociaux aient banni le contenu de QAnon de leurs platesformes, invoquant le risque de préjudice hors ligne (Roose, 2021), les théories du complot de ce mouvement continuent de circuler. Le Federal Bureau of Investigation (FBI) a averti que les théories du complot constituent une nouvelle menace de terrorisme intérieur aux États-Unis (Winter, 2019). Le département de la Sécurité intérieure des États-Unis a également lancé des avertissements concernant la montée de la violence de la part de groupes extrémistes nationaux, notamment ceux motivés par de telles théories (DHS, 2021).

Si les théories de QAnon se concentrent principalement sur les États-Unis, le Canada n'est pas à l'abri de problèmes de sécurité publique découlant de la mésinformation (encadré 4.2). Une analyse des médias sociaux a révélé que le Canada est le troisième pays en matière d'intensité du contenu de QAnon sur Twitter (Gallagher *et al.*, 2020). L'exposition à des comptes Twitter situés aux États-Unis est associée à une probabilité accrue de publier de la mésinformation sur des comptes situés au Canada (Bridgman *et al.*, 2021). Une analyse de l'environnement Web de l'extrémisme de droite a révélé que les extrémistes de droite canadiens discutent plus souvent de théories du complot non fondées et de mésinformation sur la politique américaine que sur la politique canadienne (Hart *et al.*, 2021). La même étude a constaté que le Canada était le troisième pays le plus mentionné par les extrémistes de droite en ligne aux États-Unis (Hart *et al.*, 2021).

4.3.3 Mésinformation visuelle

La mésinformation visuelle se présente sous de nombreuses formes, avec des niveaux de perfectionnement variables

Les visuels sont des outils efficaces pour formuler et souligner des questions spécifiques, ce qui se traduit par leur omniprésence dans la couverture de l'actualité et dans les médias en ligne (Powell *et al.*, 2015). Les diverses manières de créer ou de communiquer de la mésinformation visuelle peuvent rendre difficile l'évaluation de son impact sur les spectateurs, en particulier lorsqu'elle est reçue sur les médias sociaux (Powell *et al.*, 2015; Hameleers *et al.*, 2020; Brennen *et al.*, 2021). Les techniques de manipulation des images numériques sont de plus en plus accessibles (Paris et Donovan, 2019). Certains utilisent les procédés d'hypertrucage (section 3.1), dans lesquels des techniques de synthèse d'images complètes permettent de créer des images entièrement fictives, mais très réalistes (Khoo *et al.*, 2021). Notamment, de faux profils de médias sociaux comprenant des photos synthétiques d'individus inexistants ont été utilisés pour faciliter la fraude et les campagnes de mésinformation (Ajder *et al.*, 2019; Carlini et Farid, 2020). La manipulation visuelle peut également se faire par montage rudimentaire (p. ex. couper-coller) afin de partager des informations hors contexte ou de

manière intentionnellement trompeuse (Paris et Donovan, 2019; Brennen *et al.*, 2021; Khoo *et al.*, 2021).

Encadré 4.2 Les théories du complot concernant la sécurité publique au Canada

Incident à Rideau Hall : En juillet 2020, un homme armé a été arrêté après avoir enfoncé avec une camionnette la porte piétonne de Rideau Hall à Ottawa, résidence du premier ministre du Canada et de la gouverneure générale — aucun des deux n'était toutefois présent au moment de l'incident (ONCJ, 2021). Le suspect a par la suite été inculpé de 22 crimes, dont usage abusif d'armes prohibées et menaces (ONCJ, 2021). Bien que la GRC n'ait pas fait de commentaires sur les motivations exactes du suspect, les journalistes ont trouvé des publications sur QAnon et d'autres fausses théories du complot sur ses comptes de médias sociaux, dont certaines affichées peu avant l'incident (Boutilier et Ling, 2020).

Le convoi : Le convoi qui a convergé vers Ottawa en janvier 2022 a causé des perturbations massives dans la ville et a abouti à plus de 200 arrestations et à la toute première utilisation de la *Loi sur les mesures d'urgence* du Canada (Fraser, 2022; Tunney, 2022). Il s'agissait d'un mouvement complexe et multidimensionnel; alors que nombre de ses membres protestaient contre la vaccination obligatoire, des éléments substantiels s'articulaient plus généralement autour de théories du complot et d'une idéologie antigouvernementale violente considérée comme une menace pour la sécurité nationale par le SCRS (DEDC, 2022). Certains de ses dirigeants et participants soutenaient QAnon et affirmaient faussement que le Forum économique mondial avait l'intention d'imposer le totalitarisme (Ling, 2022). En partie motivés par ces griefs et ces théories du complot, les organisateurs du convoi ont rallié des partisans pour collecter des fonds sur les médias sociaux, et ont finalement alimenté un mouvement qui continue de proliférer en ligne (Ling, 2022).

La mésinformation visuelle est plus difficile à combattre que la mésinformation textuelle

L'analyse de la mésinformation visuelle exige des chercheurs et des organisations qu'ils recueillent, stockent et analysent de grosses quantités de données pour entraîner des systèmes de détection automatisés (Brennen *et al.*, 2021). De même, le contenu visuel se propage plus loin et plus vite que les capacités de détection et

de suivi des équipes de modération en ligne et des chercheurs à l'aide des outils dont on dispose (Paris et Donovan, 2019). Bien que des techniques permettant de déceler les médias manipulés s'améliorent (Rao *et al.*, 2021), les recherches et les interventions actuelles s'effectuent largement en réaction et portent sur les techniques de manipulation existantes (Paris et Donovan, 2019; Khoo *et al.*, 2021). Si les informations textuelles peuvent être trompeuses selon la manière dont elles sont interprétées, il peut être tout aussi difficile de classer les éléments visuels comme « vrais » ou « faux », car l'interprétation d'une image par le public peut varier en fonction d'un ensemble de facteurs, y compris le texte qui lui est associé (Matthes *et al.*, 2021; von Sikorski, 2021). Par exemple, lorsque des visuels réels et non modifiés sont partagés sans contexte, ou en combinaison avec des descriptions trompeuses, ils peuvent devenir viraux et provoquer la peur ou l'indignation du public (Paris et Donovan, 2019; Dan *et al.*, 2021).

Si on peut faire appel à la vérification des faits pour expliquer certaines informations visuelles erronées, le processus peut être exigeant en ressources lorsqu'une expertise spécialisée est nécessaire pour déterminer si une image a été manipulée (Brennen *et al.*, 2021; Khoo *et al.*, 2021). Il n'est pas nécessaire qu'il y ait tromperie visuelle totale pour qu'une campagne de mésinformation sème la confusion dans l'esprit du public, suscite une réaction émotionnelle ou sème la méfiance à l'égard des informations légitimes; en d'autres termes, les visuels peuvent générer de fortes réactions émotionnelles ou de l'incertitude chez les spectateurs même si ces derniers sont conscients que les informations qu'ils voient sont inexactes (Vaccari et Chadwick, 2020; Dan *et al.*, 2021). Néanmoins, s'il existe des liens clairs entre le visionnement de mésinformation visuelle et le fait d'avoir des réactions émotionnelles, on en sait moins sur la manière dont l'information visuelle est créée ou sur le degré auquel elle est utilisée pour inciter les gens à agir hors ligne (Dan *et al.*, 2021).

Même si les technologies employées pour créer, propager et déceler la mésinformation visuelle se sont améliorées ces dernières années, il n'y a pas eu de conception et d'adoption correspondantes de pratiques sociales, politiques et économiques pour lutter contre ce type de mésinformation (Paris et Donovan, 2019; Dan *et al.*, 2021). Ces mêmes platesformes de médias sociaux qui reposent sur les utilisateurs pour créer et partager du contenu ont du mal à modérer ce qui a été produit (section 4.4). En effet, avec les outils techniques et les tentatives de réglementation actuels, il est souvent difficile de savoir qui peut, ou devrait, être tenu responsable lorsque du contenu problématique est produit, partagé ou repartagé sur les platesformes.

4.4 Platesformes de médias sociaux

4.4.1 Contenu criminel

Le contenu criminel sur les platesformes de médias sociaux est en hausse

Comme nous l'indiquons dans le chapitre précédent, de nombreux crimes cyberfacilités ou comportements préjudiciables sont perpétrés sur des platesformes de médias sociaux largement autorégulées. Par exemple, une enquête menée auprès de 38 corps policiers d'Angleterre et du Pays de Galles a révélé que, au cours des trois premiers mois de confinement en raison de la COVID-19, la communication pour plus de 50 % des crimes de pédophilie s'est faite par le biais d'applications appartenant à Meta, comme Instagram, Facebook et WhatsApp, tandis qu'elle l'a été par Snapshat dans 20 % des cas (NSPCC, 2020). Cette section offre un aperçu des diverses mesures d'autorégulation prises par les entreprises de médias sociaux pour modérer, supprimer et combattre d'une manière quelconque le contenu préjudiciable sur leurs platesformes, notamment le contenu extrémiste et haineux et la mésinformation. Bien qu'on dispose de preuves d'interventions fructueuses dans certains cas, et que des méthodes nouvelles et prometteuses soient en cours de déploiement, des problèmes persistants de confiance (encadré 4.3), de transparence, de responsabilisation et de cohérence ont rendu les tentatives de modération de contenu inadéquates à ce jour. En particulier, la façon dont les platesformes choisissent de répondre à la pression populaire et leurs décisions en matière d'autorégulation peuvent mener à une incohérence et une inconstance en ce qui concerne ce qui est autorisé ou non sur les platesformes de médias sociaux (Cusumano *et al.*, 2021; Ghosh, 2021a) (encadré 4.4).

Encadré 4.3 Le peu de confiance du public dans les entreprises de médias sociaux

Malgré la popularité des platesformes de médias sociaux en tant qu'agrégateurs de nouvelles et de partage d'information, la confiance dans la capacité de ces entreprises à lutter contre la mésinformation est faible. Les résultats de l'enquête révèlent que les Canadiens « ne font pas confiance aux platesformes de médias sociaux pour agir dans l'intérêt du public » [traduction libre]. La confiance dans les platesformes de médias sociaux (p. ex. Facebook, TikTok ou WhatsApp) est plus faible que dans les compagnies pétrolières (Imperial Oil ou Shell Canada), dans les grandes entreprises technologiques (Google ou Apple) et dans les fournisseurs de télécommunications (Bell Canada). Ces résultats indiquent également que les efforts déployés par ces platesformes pour lutter contre la mésinformation (p. ex. par une meilleure vérification des faits) n'ont pas eu d'effet important sur la façon dont la population canadienne percevait les entreprises de médias sociaux entre 2019 et 2021.

(Andrey *et al.*, 2021b)

4.4.2 Contenu extrémiste

Les platesformes de médias sociaux ont pris des mesures pour supprimer le contenu extrémiste, avec des résultats mitigés

Les entreprises de médias sociaux ont pris des mesures pour lutter contre le contenu extrémiste, avec une efficacité variable. Meta, par exemple, interdit sur Facebook les groupes qui « proclament une mission haineuse et violente » et supprime le contenu qui « les représente, en font l'éloge ou les soutient » [traduction libre] (Facebook Canada, 2021). De même, environ la moitié des chaînes YouTube et des groupes Facebook privés qui présentaient ce genre de contenu en 2019 étaient devenus inactifs en 2020 (Hart *et al.*, 2021). Cependant, les chaînes et pages à contenu d'extrême droite sont souvent vite remplacées par de nouvelles, ce qui nuit actuellement à la capacité de réduire significativement ce type de support à long terme (Hart *et al.*, 2021). À l'exception de YouTube, pour laquelle les chercheurs ont observé une diminution notable du volume de contenu d'extrême droite, on a détecté davantage d'activités d'extrême droite sur les platesformes de médias sociaux en 2020 par rapport à 2019 (Hart *et al.*, 2021). À mesure que le secteur gagne en maturité, il devient de plus en plus évident que d'autres méthodes sont plus efficaces pour traiter diverses catégories de contenu. Ce constat a été fait dans une enquête menée auprès d'employés pertinents d'entreprises de médias sociaux et d'applications de messagerie, qui a révélé que si

l'analyse automatisée du contenu est considérée comme relativement efficace pour détecter le MAP connu, elle l'est moins pour détecter le contenu extrémiste ou lié au terrorisme (Pfefferkorn, 2022).

Encadré 4.4 Incitations financières et conception des platesformes de médias sociaux

Les entreprises de médias sociaux comptent parmi les entreprises les plus rentables au monde; pourtant, leur modèle économique repose en grande partie sur la fourniture de services gratuits à leurs utilisateurs. Un court-métrage de 1973 intitulé *Television Delivers People*, réalisé par les artistes Richard Serra et Carlota Fay Schoolman, laissait entendre que si un service (p. ex. la télévision) est gratuit, alors le téléspectateur doit être le produit. Cette idée a été reprise pour décrire le modèle économique sur lequel s'appuient de nombreuses entreprises de médias sociaux : fournir un service gratuit au public, dont l'attention est ensuite transmise aux annonceurs pour en tirer un bénéfice (McFarlane, 2021). Par conséquent, toute décision d'une entreprise de médias sociaux susceptible d'influencer la réaction des utilisateurs, comme la modération du contenu (p. ex. augmenter ou réduire la visibilité des messages, modifier les algorithmes utilisés pour afficher le contenu et les publicités ou bloquer ou interdire des utilisateurs), a le potentiel de nuire à sa rentabilité (Grygiel et Brown, 2019).

Autrement dit, les décisions de modération du contenu ne se limitent pas au respect d'un débat ouvert et à la sécurité des utilisateurs, elles sont également d'ordre financier — une conséquence de la conception même de nombre de ces platesformes. Pour de nombreuses entreprises, la modération du contenu est effectuée en interne ou externalisée, ce qui nécessite des ressources de l'entreprise dans les deux cas. Parallèlement, les incitations à détourner des ressources vers la modération du contenu peuvent être minimes et peu efficaces, ce qui mène à des appels à une meilleure autorégulation et à une réforme législative (Cusumano *et al.*, 2021; Ghosh, 2021a). En outre, la façon dont les utilisateurs se comportent sur les platesformes en ligne dépend du choix de conception effectué par la plateforme elle-même. Les utilisateurs se voient présenter des communautés et des services en ligne construits sur des *capacités de suggestions sociotechniques* — telles que le partage, les mentions « J'aime » ou les commentaires directs —, qui sont définies

(Continue)

(a continué)

par la relation entre l'action de l'utilisateur, la plateforme et le contexte social, ce qui peut influencer le comportement et la rétention des utilisateurs sur n'importe quelle plateforme (Leonardi et Vaast, 2016). Par exemple, Twitter permet aux utilisateurs d'« aimer » des messages (ce qui peut augmenter la fréquence à laquelle ces messages sont montrés aux autres), mais n'offre pas la possibilité de les « détester ». Ce choix de conception pourrait avoir une incidence considérable sur ce que les utilisateurs choisissent de publier, sur ce qu'ils peuvent voir et sur leur désir de continuer à utiliser la plateforme, trois paramètres qui influent sur l'attrait commercial de la plateforme pour les annonceurs.

Les entreprises de médias sociaux ont adapté leurs tactiques pour faire face aux contenus extrémistes violents. Meta, par exemple, met continuellement à jour ses politiques de modération du contenu en réponse aux conseils d'experts et autres. Depuis 2020, elle supprime le contenu négationniste et elle a élargi sa politique relative aux organisations et individus dangereux pour inclure dans sa liste ceux qui n'incitent pas directement à la violence, mais qui représentent néanmoins un risque pour la sécurité publique parce qu'ils célèbrent des actes violents (Facebook Canada, 2021). Des mesures sont prises à l'encontre de ces personnes, certaines ayant été carrément bannies de Facebook (Facebook Canada, 2021). Il semble toutefois que les décisions concernant la sécurité publique soient prises de manière ponctuelle, ce qui inquiète les groupes de la société civile quant aux critères selon lesquels les organisations ou les individus sont versés dans cette liste, certains demandant à Meta d'adopter une méthode plus systématique pour supprimer l'ensemble du contenu relevant de cette catégorie (Horwitz et Scheck, 2021). Les individus chargés des examens de modération pour les grandes entreprises de médias sociaux travaillent souvent dans de mauvaises conditions et subissent des préjudices psychologiques en raison de la nature de leur tâche, qui leur demande de visionner et de supprimer du contenu nuisible et offensant, y compris du contenu terroriste, de la plateforme qui les emploie (encadré 4.5).

Encadré 4.5 Les mauvaises conditions de travail des modérateurs de contenu

Les platesformes de médias sociaux utilisent en partie l'intelligence artificielle (IA) pour la modération du contenu, mais elles s'appuient également sur des modérateurs humains qui décident si le contenu illégal ou préjudiciable (p. ex. MAP ou contenu violent) doit être retiré (Dwoskin *et al.*, 2019; Roberts, 2019; Llansó, 2020). Une grande partie du travail de modération du contenu est confiée à des tiers situés dans le monde entier, souvent en dehors de l'Amérique du Nord, où l'on a signalé des pratiques d'exploitation de la main-d'œuvre, une rémunération inadéquate et peu de soutien face aux répercussions psychologiques de l'exposition continue à du contenu nuisible (Dwoskin *et al.*, 2019; Perrigo, 2022). Les mêmes affirmations ont aussi été faites à propos des modérateurs de contenu tiers en Amérique du Nord (Newton, 2019).

Les entreprises de médias sociaux ont lancé quelques initiatives coordonnées et autorégulées. Par exemple, le Global Internet Forum to Counter Terrorism (GIFCT) a vu le jour en 2017 sous la forme d'une collaboration entre Microsoft, YouTube, Facebook et Twitter, avant de devenir une organisation non gouvernementale (GIFCT, 2020). Le GIFCT est une organisation regroupant des entreprises technologiques qui coordonne le partage de renseignements, de recherches et de stratégies entre ses membres afin de lutter contre la propagation de contenu terroriste et extrémiste violent en ligne. Les membres ont accès à des outils conjoints, tels qu'une plateforme d'identification du contenu, le partage d'URL et un protocole commun en cas d'incident concernant le contenu. Le GIFCT finance également des recherches sur le terrorisme et la technologie et organise des séances de formation en partenariat avec d'autres organisations (p. ex. Tech Against Terrorism) (GIFCT, 2020). Cependant, certains experts juridiques ont soulevé des problèmes de reddition de comptes; ils ont notamment critiqué le fait que GIFCT n'a pas de surveillance et de transparence adéquate, car il n'existe pas de processus d'audit ou de contestation des décisions du GIFCT (Douek, 2020).

Le fait que les grandes platesformes de médias sociaux suppriment du contenu qui viole leurs normes communautaires est probablement une des principales raisons pour lesquelles de nombreux groupes extrémistes sont très actifs sur des platesformes « marginales » (Hart *et al.*, 2021). Parmi ces platesformes, les préférées sont Gab, Telegram, BitChute et Odysee, qui ont toutes une modération du contenu moins stricte que les platesformes grand public (Hart *et al.*, 2021);

des applications audio comme Clubhouse, quant à elles, permettent aux utilisateurs de communiquer au sein de clavardoirs audio donnant accès à un large public (Dwoskin *et al.*, 2021a). Telegram, une application de médias sociaux basée à Dubaï et utilisée notamment par les manifestants prodémocratie à Hong Kong et par les extrémistes islamiques, a accru son volume d'utilisateurs américains autour de l'insurrection du 6 janvier au Capitole (Molla, 2021). Les platesformes marginales jouent un rôle disproportionné dans l'incubation et l'amplification des groupes désignés comme des organisations terroristes au Canada (Hart *et al.*, 2021). On en sait beaucoup moins sur les mesures de modération prises par les plus petits sites de médias sociaux, ce qui souligne l'importance de fournir aux entreprises un soutien pour le développement de leur capacité à s'attaquer à la promotion et à la circulation du contenu extrémiste et de financer la recherche pour étudier les petits réseaux émergents (CCECPV, 2018; SECU, 2022a).

4.4.3 Contenu haineux

La manière dont les platesformes de médias sociaux modèrent le contenu haineux suscite des inquiétudes

Les entreprises, et non les États, sont les principales responsables de la détection et du contrôle du discours haineux en ligne (Ullmann et Tomalin, 2020). La plupart des grandes entreprises de réseaux sociaux, telles que Meta, Google et Twitter, ont leurs propres définitions, directives d'utilisation et politiques d'entreprise en ce qui concerne ce discours. Tel qu'elles sont actuellement conçues et mises en œuvre, ces directives et politiques ont tendance à être réactives, dans la mesure où les entreprises n'interviennent en général face aux messages haineux qu'après qu'ils ont été publiés et signalés par des utilisateurs (Ullmann et Tomalin, 2020). S'il existe des outils de suppression automatique du contenu, leur mise en œuvre se heurte à des problèmes techniques qui doivent être surmontés. Par exemple, en raison de l'existence de biais et d'un faible contexte social dans les données utilisées pour entraîner les systèmes d'IA servant à modérer le discours haineux, le contenu publié par des membres de communautés marginalisées est plus susceptible d'être étiqueté comme offensant, ce qui peut mener à la suppression excessive de contenu inoffensif (Sap *et al.*, 2019; Dias Oliva *et al.*, 2021). C'est probablement l'une des raisons pour lesquelles la plupart des entreprises ont actuellement tendance à s'en remettre à des modérateurs humains pour évaluer la majeure partie du contenu signalé et décider si ce contenu atteint le seuil de suppression (Ullmann et Tomalin, 2020).

La modération de la haine en ligne est encore compliquée par le fait que la transparence totale des pratiques des platesformes de médias sociaux est impossible. Selon Frances Haugen, ancienne employée de Meta et lanceuse

d'alerte, « presque personne en dehors de Facebook ne sait ce qui se passe à l'intérieur de Facebook. La direction de l'entreprise cache des informations vitales au public, au gouvernement américain, à ses actionnaires et aux gouvernements du monde entier » [traduction libre] (Haugen, 2021). En ce qui concerne la surveillance de la haine en ligne, des documents internes de Meta ont mis en lumière une direction hésitant à mettre en œuvre des mesures énergiques pour lutter contre le contenu haineux sur Internet au nom d'une position censée « neutre » ou « indifférente à la race » (Dwoskin *et al.*, 2021b). De plus, les archives indiquent que les algorithmes introduits en 2015 pour détecter et supprimer le discours haineux ont systématiquement échoué à supprimer le contenu mettant en danger les groupes les plus ciblés du site (Noirs, musulmans, LGBTIQ+ et Juifs). Les politiques de Meta peuvent avoir une incidence sur les utilisateurs de ses services, comme l'indique le nombre d'usagers noirs qui quittent Facebook, potentiellement en partie par crainte pour leur sécurité et leur bien-être (Dwoskin *et al.*, 2021b).

Les pratiques de collecte de données ou de surveillance peuvent également dissuader l'utilisation en ligne ou inciter les gens à s'autocensurer ou à autoréguler leur propre droit à la libre expression, ce qui a un effet paralysant (Solove, 2006). Ces pratiques de surveillance peuvent être utilisées par les forces de l'ordre ou par les entreprises elles-mêmes. Par exemple, la plupart des grandes platesformes en ligne, dont Facebook, YouTube, Twitter et Google, utilisent des systèmes de « notification et de retrait », qui permettent aux utilisateurs individuels de signaler le contenu illégal ou répréhensible (Keller, 2021). En raison de l'immense quantité de demandes de retrait reçues, les entreprises peuvent soit traiter ces demandes sans raison légale valable, soit procéder à une enquête, mais se tromper dans leur jugement — en supprimant finalement du contenu légal (Keller, 2021). Dans un cas comme dans l'autre, il peut en résulter une suppression excessive du contenu en ligne et l'hésitation des utilisateurs à publier librement et à exercer pleinement leur liberté d'expression.

4.4.4 Mésinformation et contenu trompeur

Les tactiques de suppression de la mésinformation des platesformes de médias sociaux ont eu un succès limité

La plupart des platesformes de médias sociaux ont pris certaines mesures pour lutter contre la mésinformation. Ces mesures s'efforcent souvent d'équilibrer liberté d'expression et protection contre les préjudices (p. ex. Facebook Oversight Board, 2019), mais elles ont eu un succès limité et ont soulevé de multiples préoccupations. Les platesformes de médias sociaux ont élaboré des politiques qui déterminent ce qui est considéré comme de la mésinformation et ont montré une certaine capacité à ralentir sa prolifération. Par exemple, à la suite de l'attaque sur

le Capitole en janvier 2021, Facebook a supprimé les publications, les groupes et les utilisateurs faisant la promotion des théories complotistes de QAnon, conformément à sa politique de coordination des mesures de lutte contre les préjudices et la promotion du crime (Booker, 2021). De même, Twitter a évoqué la nécessité de prendre « des mesures coercitives rigoureuses contre les comportements susceptibles de provoquer des préjudices hors ligne » [traduction libre]; la plateforme a suspendu plus de 70 000 comptes partageant le contenu de QAnon en moins d'une semaine (Twitter, 2021a).

En janvier 2019, YouTube a annoncé son intention de freiner la diffusion de vidéos « qui pourraient mésinformer les utilisateurs de manière nuisible » [traduction libre] (YouTube, 2019). Une étude portant sur 8 millions de recommandations YouTube sur une période de 15 mois a révélé que la plateforme était en mesure de réduire les recommandations vidéo de théories du complot au moyen de son algorithme (Faddoul *et al.*, 2020). Cependant, si l'intervention a presque éliminé certaines théories du complot de ses recommandations, en particulier celles concernant des sujets très médiatisés, elle a à peine influé sur d'autres (Faddoul *et al.*, 2020).

Certaines entreprises de médias sociaux ont fait appel à des groupes externes pour les aider à lutter contre la mésinformation. Par exemple, Meta et TikTok ont formé à cette fin des partenariats avec des entreprises tierces de vérification des faits (Facebook, 2020b ; Ardill, 2021). Les fausses affirmations qui n'enfreignent pas les normes communautaires de Facebook sont soumises à des partenaires indépendants de vérification des faits qui détectent, examinent et évaluent la mésinformation virale; les affirmations qui violent ses normes, comme les incitations à la violence, sont souvent supprimées par Meta elle-même (Facebook Canada, 2021). Si une entreprise de vérification des faits juge qu'un élément de contenu est faux, Facebook réduit sa diffusion, avertit les utilisateurs qui essayent de le partager (ou qui l'ont déjà partagé) et appose une étiquette d'avertissement avec un lien vers l'article du vérificateur de faits réfutant la fausse affirmation (sauf dans des cas particuliers où il est supprimé, comme expliqué ci-dessous). Meta utilise également l'automatisation, par exemple l'IA, pour détecter et supprimer les faux comptes (Facebook Canada, 2021), mais il est prouvé que la vérification des faits automatique doit être complétée par des vérificateurs de faits humains pour éviter la suppression excessive de contenus non nuisibles (OCDE, 2020b).

Les données probantes révèlent que la vérification des faits à elle seule n'est pas une solution miracle (Tenove et Tworek, 2019). Une étude expérimentale a constaté que l'ajout d'avertissements au titre des nouvelles identifiées comme fausses par des vérificateurs de faits tiers « entraîne une réduction modeste de la perception d'exactitude des faux titres » [traduction libre] (Pennycook *et al.*, 2020). Cependant, les faux titres qui n'ont pas été signalés ont été perçus comme « validés » et plus exacts que les titres de contrôle, et leur partage sur les médias

sociaux a donc été davantage envisagé. Des recherches ultérieures indiquent qu'une façon d'améliorer la qualité du contenu partagé peut consister à inciter les utilisateurs à faire attention à l'exactitude (p. ex. en leur envoyant un message sur Twitter leur demandant leur avis sur l'exactitude d'un titre) (Pennycook *et al.*, 2021). En plus de la vérification des faits, certaines platesformes de médias sociaux ont demandé l'avis et les conseils de groupes consultatifs ou de comités d'examen indépendants à propos de l'élaboration et de la mise en œuvre de politiques sur la modération de contenu (encadré 4.6).

Encadré 4.6 Conseil de surveillance de Meta

Un exemple notable de groupe d'examen indépendant du contenu en ligne est le conseil de surveillance mis sur pied par Meta. Il est composé d'experts du monde entier qui examinent certains cas concernant les décisions de modération de contenu prises par Meta, puis fournissent des décisions contraignantes que « Facebook mettra en œuvre [rapidement], sauf si la mise en œuvre [...] pourrait enfreindre la loi » [traduction libre] (Facebook Oversight Board, 2019). Ce conseil est censé agir comme une sorte de tribunal des jugements, bien qu'il ait soulevé des critiques sur sa structure et sa composition, sur la question de savoir s'il peut vraiment être indépendant de Meta et s'il peut s'attaquer adéquatement à l'ampleur et à la diversité du contenu de Facebook (Klonick, 2020).

Le conseil de surveillance a notamment examiné les commentaires du président américain de l'époque, Donald Trump, sur Facebook et Instagram pendant les émeutes du 6 janvier au Capitole et la décision ultérieure de Meta de supprimer ces commentaires et de suspendre le compte du président (Facebook Oversight Board, 2021). Le comité a confirmé la décision de Meta de bloquer l'accès à ce compte, mais a jugé que la « suspension indéfinie » n'était pas appropriée et a déclaré que Meta devait être transparente quant aux « règles qu'elle suit lorsqu'elle impose des sanctions à l'échelon du compte contre des utilisateurs influents » [traduction libre], imposer (et expliquer) des suspensions limitées dans le temps et évaluer si le risque « s'est atténué avant la fin de la suspension » [traduction libre], entre autres recommandations (Facebook Oversight Board, 2021).

Les politiques de suppression de contenu sont incohérentes d'une plateforme à l'autre et la modération manque de ressources

Certains experts ont fait valoir que les mesures prises par les entreprises de médias sociaux à ce jour n'ont pas suffi à endiguer la propagation de gros volumes de mésinformation (Bellemare et Ho, 2020). Comme dans le cas du discours haineux, une critique courante est que ces mesures sont généralement réactives et ne sont pas uniformes entre les platesformes (Heer *et al.*, 2021). Chaque plateforme décide de ce qui est considéré comme de la mésinformation et détermine l'intervention adéquate. Meta, par exemple, autorise généralement la mésinformation politique, mais en a par le passé réduit la place dans les fils d'actualité de Facebook, a supprimé la mésinformation concernant la COVID-19 si elle « pouvait causer des dommages physiques imminents » [traduction libre] (Facebook, 2020b) et a interdit la mésinformation relative au vote (p. ex. la publication de fausses heures de vote) (Leinwand, 2018). Twitter, quant à elle, a utilisé une échelle progressive d'options allant de l'étiquetage d'un gazouillis comme trompeur ou sensible jusqu'à sa suppression, voire à la suspension du compte associé (Twitter, 2021b). Autrement dit, du contenu diffusé sur une plateforme peut faire l'objet d'un « bannissement furtif » (ou *shadow ban*, méthode consistant à bloquer un utilisateur d'une plateforme à son insu, habituellement en rendant ses publications invisibles aux autres utilisateurs) sur une autre, ou entraîner la fermeture du compte sur une troisième. Par conséquent, il n'y a pas de prévisibilité pour les utilisateurs et, comme les politiques peuvent être rapidement modifiées, il peut être difficile pour les organismes de réglementation et les chercheurs de comparer directement et systématiquement les politiques des entreprises.

La langue de la mésinformation a une incidence sur la probabilité qu'elle soit détectée. Il y a trop peu de modérateurs humains possédant les compétences linguistiques et connaissant le contexte culturel local nécessaires pour déceler et supprimer le contenu Facebook préjudiciable et faux d'utilisateurs de plusieurs pays en développement; si les systèmes d'IA peuvent aider, ils ne sont pas efficaces contre de nombreuses langues employées par les utilisateurs de Facebook (Culliford et Heath, 2021; Scheck *et al.*, 2021). Plus de 90 % des usagers mensuels de Facebook se trouvent en dehors des États-Unis et du Canada; pourtant, sur les 3,2 millions d'heures consacrées à la suppression ou à l'étiquetage de faux contenu en 2020, les employés et soustraitants de Meta n'ont consacré que 13 % de ce temps à du contenu non américain (Scheck *et al.*, 2021). La capacité linguistique limitée des modérateurs nuit au Canada, étant donné que 12 % des personnes dans le pays parlent principalement une langue autre que l'anglais ou le français à la maison (StatCan, 2018) et que les nouveaux arrivants sont ciblés par des campagnes de mésinformation en ligne dans des langues non officielles (Edmonds et Flahault, 2021).

Le chiffrement et le manque de transparence constituent des défis constants pour les entreprises de médias sociaux

Les platesformes qui chiffrent les messages, comme WhatsApp, peuvent avoir plus de mal à surveiller la mésinformation, car elles ne peuvent pas lire les messages personnels (Gupta et Taneja, 2018). Cependant, une étude a montré que les platesformes de médias sociaux et les applications de messagerie ont tendance à s'appuyer sur des outils de signalement des abus d'utilisateurs pour lutter contre la mésinformation, ainsi que sur des métadonnées telles que les noms d'utilisateur des comptes, la fréquence ou le volume de l'activité sur les comptes et les signalements antérieurs d'abus, plutôt que d'accéder au contenu envoyé entre usagers, qu'il soit chiffré ou non (Pfefferkorn, 2022). Certains chercheurs se sont interrogés sur les mesures mises en place par les entreprises de médias sociaux; par exemple, les services de messagerie ne sont pas particulièrement transparents — et donc compréhensibles pour les utilisateurs — et l'efficacité des mesures adoptées est souvent peu claire (Heer *et al.*, 2021). Accorder aux chercheurs indépendants un plus grand accès aux données des entreprises de médias sociaux permettrait une évaluation indépendante des affirmations de ces entreprises, même s'il sera aussi nécessaire d'établir des politiques garantissant la confidentialité ou la sécurité des utilisateurs et des platesformes (Tenove et Tworek, 2019).

Les grandes platesformes de médias sociaux peuvent réduire la propagation de la mésinformation, mais pas l'éradiquer

Les efforts déployés par les entreprises de médias sociaux pour empêcher la propagation de théories du complot et autres types de mésinformation peuvent avoir des conséquences inattendues. Si les avis divergent quant à l'efficacité à long terme de l'interdiction des comptes sur les sites grand public, les données probantes soulignent les inconvénients notables de ce genre de tactique. En particulier, les mesures visant à supprimer la mésinformation et d'autres types de contenu en ligne nuisibles peuvent pousser les producteurs d'un tel contenu à se déplacer vers des platesformes et des sites marginaux. Après l'attaque sur le Capitole en janvier 2021, Facebook, Twitter et YouTube ont interdit des milliers de comptes faisant la promotion de QAnon, mais la théorie du complot a persisté parce que ses adeptes ont migré vers des sites tels que Gab et Telegram (Bond, 2021).

Il est plus difficile de contrôler la propagation des théories du complot sur les sites marginaux et, une fois sur ces sites, les gens peuvent être exposés à du contenu encore plus extrémiste et potentiellement se radicaliser davantage (Bond, 2021) (section 3.2). Parallèlement, il a été démontré que la suppression de comptes majeurs et comptant un grand nombre d'adeptes réduisait considérablement la propagation de la mésinformation sur les médias sociaux en quelques jours

(Ghosh, 2021b). Une étude réalisée sur ces inconvénients a révélé que deux communautés bannies de Reddit ayant migré vers des sites marginaux ont connu une réduction globale des messages, des utilisateurs actifs et des nouveaux utilisateurs, bien que les utilisateurs qui sont restés aient eu tendance à générer du contenu présentant une toxicité et une radicalisation accrues (Horta Ribeiro *et al.*, 2021).

4.5 Tactiques préventives

4.5.1 Éducation à la culture numérique

Un ensemble de programmes prometteurs cherchent à améliorer la littératie numérique

Outre les mesures prises par les entreprises de médias sociaux (section 4.4) et les outils réglementaires (chapitre 5), inculquer aux gens des compétences numériques, médiatiques et informationnelles peut leur procurer les moyens d'évaluer de manière plus critique les informations en ligne, de déceler le contenu haineux et la mésinformation, de rechercher des sources d'informations crédibles et de réduire le risque d'être victime de crimes cyberfacilités (OCDE, 2020b; CPVP, 2022). Le gouvernement du Canada a financé 50 initiatives d'éducation lancées par des universités et des organismes non gouvernementaux pour lutter contre la mésinformation en ligne (De Coninck *et al.*, 2021). L'Organisation de coopération et de développement économiques (OCDE, 2020b) note que des partenariats étroits entre les platesformes de médias sociaux, les gouvernements, les médias d'information et les éducateurs sont essentiels au succès de ces initiatives.

Les outils éducatifs destinés à améliorer la littératie numérique peuvent se révéler efficaces. Une étude a constaté que les interventions d'éducation aux médias numériques auprès d'un échantillon national représentatif d'Américains ont permis d'améliorer de 27 % le discernement entre les nouvelles véridiques et fausses (Guess *et al.*, 2020). La recherche a également montré que si la littératie informationnelle — la capacité à trouver des informations en ligne qui sont vérifiées et fiables — peut augmenter de manière significative la probabilité de déceler les fausses nouvelles, la littératie numérique ou médiatique seule ne suffit pas (Jones-Jang *et al.*, 2021). Au Canada, une initiative éducative qui s'est révélée efficace est le programme CTRL-F : Dans les faits de CIVIX. Le programme enseigne aux jeunes à évaluer les informations en ligne avec les mêmes techniques de lecture latérale que celles utilisées par les vérificateurs de faits (CIVIX Canada, 2022). Ces techniques consistent à effectuer de simples recherches sur le Web pour trouver le contexte principal des sources et des affirmations à évaluer, au lieu de se concentrer sur l'analyse de la source d'information elle-même. Une étude portant sur plus de 2 000 élèves de la 7^{e} à la 12^{e} année, réalisée

par des évaluateurs indépendants, a révélé que les élèves ayant suivi le programme étaient plus de trois fois plus susceptibles de lire latéralement qu'un groupe témoin (Pavlounis *et al.*, 2022). La capacité des étudiants de CTRL-F à évaluer avec exactitude la fiabilité des sources et des affirmations est passée de 47 % à 75 % après avoir suivi le programme (Pavlounis *et al.*, 2022).

D'autres initiatives visent également les jeunes. HabiloMédias (anciennement Réseau Éducation-Médias) est un organisme canadien qui se concentre sur l'enseignement de la culture médiatique et numérique depuis 1996, au Canada comme dans le monde (Titley *et al.*, 2014). La clé de la littéracie numérique est de faire comprendre aux jeunes utilisateurs qu'Internet n'a pas de contrôleur et que, par conséquent, les informations inexactes sont aussi largement accessibles que les informations exactes. L'éducation aux médias numériques vise à inculquer des compétences qui permettent aux jeunes de distinguer la qualité et la vérifiabilité des documents sur le Web, de réfléchir de manière critique aux sources et aux messages et de reconnaître les signaux d'alarme associés aux sources qui tentent de manipuler ou de fournir des informations biaisées (HabiloMédias, s.d.). En outre, elle peut être utile pour enseigner des méthodes efficaces pour contrer le discours haineux en ligne sans l'intensifier ainsi que pour signaler le contenu nuisible, répréhensible ou haineux (HabiloMédias, s.d.).

Afin de promouvoir la littéracie numérique, le Commissariat à la protection de la vie privée du Canada (CPVP) a créé des ressources éducatives destinées aux jeunes, dont un roman graphique, dans le but de les aider à réduire les risques d'atteinte à leur vie privée (CPVP, 2022). L'approche du CPVP consiste à aider les jeunes « à acquérir les compétences qui leur permettront d'évaluer les situations de façon éclairée par eux-mêmes », plutôt que d'imposer des règles ou des outils numériques pour bloquer l'accès au contenu (CPVP, 2022).

4.5.2 Redirection et blocage du contenu

Les outils numériques peuvent servir à réorienter les personnes susceptibles de s'engager dans des activités criminelles

Des outils numériques qui surveillent les recherches ont été utilisés pour tenter d'empêcher les utilisateurs d'accéder à du matériel illégal ou nuisible. Par exemple, un message d'avertissement contextuel peut apparaître lorsqu'une personne tape des mots-clés identifiés comme étant reliés au MPA dans son moteur de recherche (Edwards *et al.*, 2021). Dans des avertissements clairement énoncés, les utilisateurs sont informés que la visualisation de MAP est illégale. L'intensité des fenêtres d'avertissement augmente avec la gravité des termes recherchés. Ces messages sont destinés à annihiler le sentiment de sécurité et d'anonymat de l'utilisateur et, surtout chez les délinquants précoces, à dissuader

et à influencer le comportement (Edwards *et al.*, 2021). Si ces avertissements constituent une solution économique, des recherches supplémentaires sont nécessaires pour déterminer leur effet dissuasif (Prichard *et al.*, 2022). Le Centre canadien d'engagement communautaire et de prévention de la violence, qui mène le travail de lutte contre la radicalisation du gouvernement fédéral (SP, 2019a), a également conçu des outils qui redirigent les utilisateurs en fonction de leur historique de recherche (encadré 4.7).

Encadré 4.7 Canada Redirect : campagnes de contre-contenu ciblées

Moonshot (une entreprise technologique en démarrage) a lancé en 2019 Canada Redirect, grâce à l'aide financière du Fonds de résilience communautaire et en collaboration avec le Centre canadien d'engagement communautaire et de prévention de la violence. Axé sur le contenu de Daesh, d'Al-Qaïda et d'extrême droite qui incite à la violence et promeut les théories du complot, Canada Redirect a ciblé les personnes sensibles aux messages extrémistes d'après leurs recherches sur Google et « a redirigé des milliers d'entre elles vers des vidéos qui sapent les thèmes concernés ou le contenu propre à chaque recherche » [traduction libre]. Les vidéos offraient « un contenu contextuel, crédible et sûr, qui remettait en question les croyances extrémistes » [traduction libre]. Par exemple, les vidéos tentaient de susciter les émotions et l'empathie des spectateurs, soulignaient la culture toxique au sein des groupes extrémistes et mettaient en lumière l'importance du dialogue et de la diversité au Canada.

Le projet a mené des campagnes localisées, qui ont permis à Moonshot de recueillir des données à l'échelle du quartier sur l'activité de recherche extrémiste, de tester des messages et d'étudier la possibilité de fournir aux utilisateurs à risque un contenu sain et un accès à des services communautaires. Entre février 2019 et mars 2020, Moonshot a saisi 171 382 recherches par mots-clés liées à du contenu extrémiste au Canada, en anglais, en français et en arabe. Elle a enregistré 2 583 clics sur le contenu de remplacement personnalisé et 3 960 visionnages de vidéos. Les utilisateurs qui recherchaient des informations sur du contenu violent d'extrême droite étaient plus susceptibles de s'intéresser au contenu de remplacement de Moonshot.

(Moonshot CVE, 2021)

Comme indiqué à la section 4.4, les platesformes de médias sociaux ont également commencé à introduire des avertissements à l'intention des utilisateurs, dans le but de limiter la propagation de la mésinformation. Par exemple, lorsque les utilisateurs de Twitter tentent de partager un article qu'ils n'ont pas lu, un avertissement les encourage à lire l'article au préalable (Vincent, 2020; Ghaffary, 2021). Le but est d'inciter les gens à réfléchir à ce qu'ils partagent (Vincent, 2020; Ghaffary, 2021).

Le blocage et la mise en quarantaine du contenu peuvent empêcher les utilisateurs d'accéder à du contenu illégal ou préjudiciable

La *technologie Cleanfeed* regroupe divers systèmes de filtrage du contenu au niveau des fournisseurs d'accès Internet (FAI). Conçue au Royaume-Uni en 2003, elle a été introduite en 2004 et adoptée au Canada en 2006 (Brighton, 2004; Cyberaide.ca, 2022a). À sa création, Cleanfeed Canada avait pour but de bloquer l'accès aux sites Web étrangers hébergeant du MAP. Cyberaide.ca — l'organisme de réglementation désigné du Canada, administré par le Centre canadien de protection de l'enfance (CCPE) — avait alors fourni une première liste de sites bloqués, qui a par la suite été transmise aux FAI participants (Cyberaide.ca, 2022a). La participation des FAI était volontaire et il est utile de noter qu'ils n'ont eu aucune influence sur la constitution de cette liste et ne savaient pas quels sites y figuraient (Cyberaide.ca, 2022a). Aujourd'hui, la liste est tenue à jour par Projet Arachnid, au moyen de son interface de protocole d'application (API) Shield (Projet Arachnid, 2022). L'adoption de Cleanfeed a été proposée en Australie en 2008, mais une forte opposition pour des raisons de censure et de liberté d'expression a entraîné l'annulation discrète du projet en 2010 (Liebhardt, 2008). Bien que Cleanfeed Canada puisse être considérée comme une forme de censure par certains, le fait que l'accès au MAP soit illégal distingue, selon Geist (2021a), ce programme de la censure de documents considérés comme de l'expression libre.

On a aussi proposé la mise en quarantaine comme mécanisme simple de protection des utilisateurs contre l'exposition à la haine en ligne. Cette méthode de rechange à la modération humaine du contenu s'appuierait sur des systèmes de détection automatisés semblables à ceux déjà utilisés pour lutter contre les logiciels ou les courriels malveillants. La mise en quarantaine concernant la haine en ligne maintiendrait les messages douteux dans des limbes, en les marquant comme n'étant ni autorisés ni interdits (Ullmann et Tomalin, 2020). Les destinataires ou les modérateurs des messages seraient alertés de la présence d'éléments en quarantaine et auraient la possibilité de voir le message ou de le supprimer immédiatement, ce qui donnerait aux destinataires la possibilité de choisir leur propre niveau de protection. Dans un tel scénario, les expéditeurs

écrivent ce qu'ils veulent, mais les destinataires décident de ce qu'ils souhaitent voir. Selon Ullmann et Tomalin (2020), la quarantaine peut constituer un juste milieu entre la lutte contre la haine en ligne et la protection du droit à la liberté d'expression.

4.6 Résumé

Afin de répondre à la question du commanditaire sur les défis créés par les progrès des TIC en matière de prévention des méfaits en ligne, d'enquête et de poursuites, le comité d'experts a axé ce chapitre sur les platesformes Web émergentes, telles que les sites de sociofinancement et d'échange de cryptomonnaies, le Web clandestin, les RPV et les médias sociaux, qui peuvent tous servir à amplifier les méfaits, notamment les crimes graves. Bien que ces outils habilitants ne soient pas illégaux, ils peuvent faciliter le financement, la dissimulation et la propagation de contenu préjudiciable. Les cryptomonnaies, par exemple, sont largement décentralisées et peuvent être employées pour régler anonymement des transactions transfrontalières illégales et blanchir de l'argent.

Le comité d'experts a constaté que les forces de l'ordre se heurtent à d'importants écueils lorsqu'elles tentent de retracer certains échanges de cryptomonnaies, ce qui entrave les enquêtes criminelles. De même, l'anonymat offert par le Web clandestin et les outils d'occultation des données tels que les RPV peuvent protéger les personnes engagées dans des activités en ligne bénéfiques (p. ex. les journalistes) tout comme celles qui désirent nuire (p. ex. les personnes qui effectuent des ventes illicites ou partagent du MAP). Le comité d'experts a constaté que ces outils peuvent gêner la détection et l'investigation des activités criminelles et mettent en danger des utilisateurs bien intentionnés lorsqu'ils sont utilisés de manière inappropriée.

Bien que certaines pratiques aient été implantées dans le but d'améliorer la santé globale de l'écosystème numérique, le comité d'experts a relevé que leur effet reste limité, puisque le contenu nuisible continue de proliférer et que des outils en ligne continuent d'être utilisés pour faciliter les activités illégales. La mésinformation se répand en ligne plus rapidement que jamais. Même si elle n'est pas criminelle, il a été démontré qu'elle motive les crimes hors ligne et est de plus en plus liée à l'extrémisme et à la haine. Les entreprises de médias sociaux ont pris certaines mesures d'autorégulation pour modérer le contenu nuisible sur leurs platesformes, notamment le retrait de la mésinformation, mais il subsiste des problèmes de transparence, de reddition de comptes et de cohérence. Le comité d'experts a également constaté que certaines tactiques de modération ont des effets imprévus, comme la suppression excessive de contenu bénin.

Allant au-delà des défis de l'autorégulation analysés dans ce chapitre, le chapitre 5 se concentre sur la gamme d'instruments réglementaires que les différents ordres de gouvernement au Canada et à l'étranger emploient, ou envisagent, pour régir les espaces numériques et contrer les méfaits en ligne face à des TIC en constante évolution.

5

Contexte et outils réglementaires

Constatations du chapitre

- La vitesse de l'évolution technologique rend difficiles l'interprétation et l'application de la loi, et la plupart des lois canadiennes portant actuellement sur les crimes cyberfacilités ont été pensées à l'origine pour des infractions hors ligne.
- La gouvernance étatique des espaces numériques tente de concilier la protection des utilisateurs contre les crimes cyberfacilités et les libertés et droits constitutionnels, tels que la liberté d'expression et le droit à la vie privée.
- La gouvernance étatique des espaces numériques tente de dissuader les individus de mener des activités criminelles et, lorsqu'une personne est victime d'un crime cyberfacilité, cherche à faciliter les enquêtes et les poursuites sans porter indûment atteinte aux droits garantis par la Charte.
- Les gouvernements au Canada et dans d'autres pays étudient et appliquent un ensemble d'approches réglementaires pour lutter contre le crime cyberfacilité et les cyberméfaits. Il est nécessaire de prendre en compte les différences entre les systèmes juridiques et entre les cultures juridiques pour évaluer dans quelle mesure les méthodes étrangères conviennent au contexte canadien.
- La gouvernance des espaces numériques ne se limite pas aux règles et outils sanctionnés par l'État. Une variété de méthodes et d'instruments (p. ex. politiques d'autogouvernance des entreprises, codes de conduite des utilisateurs) peuvent être envisagés lors de la création d'un système de gouvernance adaptatif.

Les technologies de l'information et des communications (TIC) sont régulièrement utilisées pour faciliter les comportements criminels ou préjudiciables. Face à cela, le gouvernement canadien, comme les gouvernements étrangers, a intensifié ses efforts pour renforcer la sécurité de l'écosystème numérique. Il est possible d'atténuer ou de prévenir, au moins partiellement, les méfaits cyberfacilités au moyen d'un ensemble d'instruments juridiques, comme des lois, des règlements et des politiques. Toutefois, d'importantes questions subsistent quant à l'efficacité des réponses juridiques sanctionnées par l'État et à leur capacité à tenir compte à la fois de la protection des utilisateurs contre les méfaits cyberfacilités et de leurs libertés et droits constitutionnels, comme la liberté d'expression ou le droit à la vie privée. Dans ce

chapitre, le comité d'experts évalue un certain nombre d'instruments nationaux, étrangers et internationaux afin d'esquisser différentes approches pour lutter contre ces méfaits, tout en signalant les limites de certaines d'entre elles.

Le présent chapitre commence par un examen des lois et politiques canadiennes actuelles afin de résumer les instruments dont on dispose pour traiter ou prévenir les méfaits cyberfacilités, y compris les infractions criminelles. Il examine ensuite les politiques et les lois que d'autres pays ont proposées ou adoptées, dont certaines pourraient combler les lacunes des régimes réglementaires du Canada ou constituer une solution pour renforcer les politiques existantes. Le comité d'experts s'y penche en particulier sur certaines lois adoptées ou proposées en Australie, en Allemagne, en Nouvelle-Zélande, au Royaume-Uni et aux États-Unis, ainsi que dans l'Union européenne. Ces États ont été choisis en raison de leur lien avec le Canada en vertu d'une coopération internationale étroite (p. ex. G7 ou Groupe des cinq) et de similitudes sociopolitiques ou parce qu'elles ont introduit ou promulgué des politiques et des lois qui semblent influencer le paysage réglementaire national.

Après avoir examiné les différentes réponses étrangères aux activités nuisibles cyberfacilitées, le comité d'experts analyse l'efficacité de la collaboration internationale entre les alliés du Canada. Ce faisant, il constate que le recours au secteur privé est un élément important de la gouvernance internationale et que les propositions internationales peuvent avoir un effet paralysant sur le droit à la liberté d'expression ou porter atteinte au droit à la vie privée.

Le chapitre se termine par l'examen de l'éventail des politiques et des réformes législatives proposées par le gouvernement du Canada afin de mettre en évidence sa portée excessivement large et son interférence potentielle avec les droits constitutionnels. Par conséquent, le comité d'experts estime que l'un des principaux défis de la gouvernance étatique des espaces numériques est d'améliorer la santé de l'écosystème numérique tout en respectant les libertés et droits constitutionnels.

5.1 Sélection de lois et de politiques canadiennes

La capacité des organismes de sécurité publique à protéger la population contre les méfaits cyberfacilités dépend, en partie, des lois et des politiques que ces organismes sont chargés d'appliquer. Lorsque la réforme législative est régulièrement en retard sur la technologie, les organismes de sécurité publique, tels que les forces de l'ordre ou les organismes de réglementation, peuvent être entravés dans leur capacité à atténuer certains types de comportements criminels ou préjudiciables.

Dans cette section, le comité d'experts étudie le régime réglementaire de sécurité publique numérique sous l'angle des lois et des politiques canadiennes, afin de mettre en évidence le fait que l'évolution technologique crée plusieurs types courants de difficultés juridiques, notamment : (i) le besoin de lois contraignant ou stimulant le développement technologique; (ii) l'ambiguïté dans l'application des règles juridiques; (iii) la portée des règles juridiques actuelles et (iv) « la désuétude des règles juridiques existantes » [traduction libre] (Bennett Moses, 2007). Plus précisément, le comité d'experts se penche sur des éléments du *Code criminel* canadien, du droit civil du Québec, de la common law concernant les délits pour cause d'infraction, de la législation sur la protection de la vie privée, du droit relatif à la diffamation, des lois sur le blanchiment d'argent et de la législation antipourriel, dans le but de cerner les lacunes et les défis juridiques.

5.1.1 Répartition des pouvoirs législatifs dans le système fédéral de gouvernement du Canada

La répartition des pouvoirs législatifs entre les différents ordres de gouvernement — du fédéral au municipal — est au cœur de tout système fédéral, y compris du système canadien (Brideau et Brosseau, 2019). Ainsi, certaines questions examinées dans le présent rapport relèvent de la compétence fédérale, tandis que d'autres sont réglementées par les provinces ou les territoires, ou par une combinaison de lois et de règlements de différents ordres de gouvernement.

L'article 91 de la *Loi constitutionnelle de 1867* établit la compétence exclusive du Parlement du Canada en matière de droit criminel (Brideau et Brosseau, 2019). Ainsi, les infractions criminelles sont fixées à l'échelon fédéral et sont cohérentes dans tout le pays. Le paragraphe 92(14) de cette même loi confère toutefois aux provinces les pouvoirs en matière d'administration de la justice; cela signifie que l'application du *Code criminel* — par exemple, mener des enquêtes, porter des accusations et intenter des poursuites — relève généralement de la compétence provinciale (Brideau et Brosseau, 2019). Par conséquent, le traitement des infractions n'est pas uniforme dans tout le pays et reflète les tendances et les défis régionaux. Par exemple, la procédure de dépôt d'accusations et la durée médiane des procédures (calculée à partir de la date de la première comparution devant un tribunal jusqu'à la date de la décision finale) varient à travers le Canada (JUS, 2012; LCJC, 2017).

Le Parlement du Canada a le mandat constitutionnel de légiférer sur les échanges et le commerce en vertu du paragraphe 91(2) de la *Loi constitutionnelle de 1867*, tandis que les gouvernements provinciaux ont compétence sur la propriété et les droits civils en vertu du paragraphe 92(13) (Nisker, 2006). Malgré leurs mandats constitutionnels différents, les législateurs fédéraux et provinciaux adoptent souvent des lois sur des questions similaires (section 5.1.4). Enfin, le droit de la

responsabilité délictuelle et le droit civil contiennent d'importantes protections de la vie privée et des cadres de responsabilité. Toutefois, comme ces domaines du droit relèvent de la compétence des provinces, il existe des différences dans les recours offerts aux victimes et aux survivants de méfaits cyberfacilités au pays (section 5.1.3).

5.1.2 Le Code criminel

Quand on examine le *Code criminel* du Canada, il est évident que la plupart des actes étudiés au chapitre 3 constituent de possibles infractions criminelles. Par exemple, dans la catégorie de l'exploitation, du harcèlement et de l'abus, la diffusion non consensuelle d'images intimes est une infraction en vertu du paragraphe 162.1 (1) (encadré 5.1), tandis que le cyberharcèlement et le cybertraquage sont des infractions en vertu de l'article 264.

Encadré 5.1 Diffusion non consensuelle de contenus intimes

De novembre 2009 à février 2012, Aydin Coban, un résidant des Pays-Bas de 35 ans coupable de sextorsion s'est « cruellement et implacablement acharné » sur une adolescente canadienne, Amanda Todd, qui avait 12 ans lorsque les abus ont commencé (BCSC, 2022). Pendant plus de deux ans, il a utilisé 22 pseudonymes sur différentes platesformes de médias sociaux pour attirer sa victime ou la soumettre à de l'extorsion pour qu'elle accomplisse des actes explicites sur webcaméra en la menaçant de diffuser du contenu intime déjà en sa possession. Et quand Amanda Todd a refusé de se conformer à ses exigences, M. Coban a tenu sa promesse et a distribué des documents illicites (BCSC, 2022). Bien que le harcèlement ait été signalé à la GRC, les forces de l'ordre de l'époque n'ont pas pu le retrouver (Little, 2022). Amanda Todd s'est suicidée en 2012.

Une enquête approfondie n'a été lancée qu'après la mort de la jeune fille, et il a fallu plusieurs années pour traduire l'auteur en justice (CIGI, 2021). En 2022, la Cour suprême de la Colombie-Britannique a déclaré Aydin Coban coupable de plusieurs chefs d'accusation, notamment de possession de pornographie infantile, d'extorsion, de harcèlement criminel et de leurre d'enfant. Il a été condamné à 13 ans de prison. Selon la cour, ses actes criminels ont causé « un profond préjudice émotionnel et psychologique » à Amanda Todd et « ont incontestablement contribué à sa mort par suicide » [traduction libre] (BCSC, 2022).

(Continue)

(Continue)

En 2015, en partie en réponse au tollé suscité par cette affaire, le gouvernement fédéral a modifié le *Code criminel* en criminalisant la diffusion non consensuelle d'images intimes et en offrant plusieurs voies juridiques pour protéger les victimes et les survivants (GC, 1985; Macaulay, 2021). Entre autres choses, un contrevenant peut se voir interdire « d'utiliser Internet ou tout autre réseau numérique, à moins de le faire en conformité avec les conditions imposées par le tribunal » (GC, 1985).

De même, certaines formes de contenu répréhensible sont visées par les articles 318 et 319 de ce même *Code criminel*, qui érigent en infraction le fait de prôner le génocide, d'inciter à la haine contre un « groupe identifiable » qui est « susceptible d'entraîner une violation de la paix » et de faire des déclarations dans lesquelles il « fomente volontairement la haine contre un groupe identifiable » dans un lieu public (GC, 1985).

Le droit criminel ne tient pas toujours pleinement compte de l'expérience des femmes et des filles victimes ou survivantes de la violence facilitée par la technologie

Les recherches menées par Bailey et Mathen (2019) ont permis de recenser 410 affaires criminelles signalées au Canada concernant des actes de violence facilités par la technologie (p. ex. voyeurisme, extorsion) à l'encontre de femmes et de filles en janvier 2019. La grande majorité (91 %) des accusés dans ces affaires étaient des hommes. L'analyse de ces cas a révélé que les réponses judiciaires ne tenaient pas toujours pleinement compte de l'expérience des victimes et des survivantes à cause de deux contraintes (Bailey et Mathen, 2019). La première est la tendance à faire peser sur les femmes la responsabilité d'éviter les violences tant sexuelles que physiques (également connue sous le nom de *responsabilisation* des femmes pour leurs attaques) (Grant, 2015). La capacité du droit criminel à reconnaître l'expérience des survivantes et des victimes peut dépendre du fait que les tribunaux considèrent qu'une victime ou une survivante « mérite » d'être protégée (Bailey et Mathen, 2019). Dans certains cas, les tribunaux étaient plus enclins à qualifier la violence sexuelle contre des filles de préjudice public que la violence contre des femmes. En outre, certaines analyses judiciaires se sont concentrées sur les victimes ou les survivantes considérées comme « innocentes » ou « bonnes ». Cela signifie que, pour certaines femmes, l'incapacité d'être perçue

comme une « bonne victime » peut conduire à transférer la responsabilité de la violence sur la victime ou la survivante elle-même (Bailey et Mathen, 2019).

La deuxième contrainte à la capacité du droit criminel à pleinement tenir compte de l'expérience des victimes et des survivantes est liée aux interprétations strictes par les tribunaux de ce qu'est un *méfait* ou un *préjudice* et de la *violence* (récit 3). Le droit criminel ne reconnaît pas toujours que les univers numérique et concret forment un continuum dans lequel des commentaires et des messages sur Internet fragmentés et apparemment inoffensifs peuvent être perçus comme menaçants par les victimes (Bailey et Mathen, 2019). Lorsque le système de justice pénale ne perçoit pas pleinement le lien entre le discours en ligne et ses effets hors ligne, les victimes et les survivantes de crimes peuvent être incapables d'obtenir justice.

Récit 3 *R. c. Corby*

En 2012, la Cour provinciale de la Colombie-Britannique a rendu une décision dans l'affaire *R. c. Corby* (BCPC, 2012). Dans cette affaire, l'accusé, Wayne Corby, a été inculpé de harcèlement criminel à l'encontre de Mihaela Michelle Bogdan en vertu du paragraphe 264(1) du *Code criminel*. Selon l'accusation, M. Corby a eu un comportement qui a amené M^{me} Bogdan à craindre raisonnablement pour sa sécurité après la séparation du couple. Alors qu'il suivait M^{me} Bogdan à travers le pays, M. Corby voulait qu'elle sache qu'il n'était pas loin et a affiché plusieurs publications sur sa page Facebook, notamment des photos des endroits qu'elle fréquentait régulièrement (p. ex. lieu de travail, salle de conditionnement physique, café), ainsi que des commentaires exprimant sa nostalgie (« Tu me manques, Michelle, beaucoup ») et un lien vers la chanson de Police *Every Breath You Take*, qui décrit une personne surveillant constamment une autre (BCPC, 2012).

Bien que M. Corby ait finalement été reconnu coupable de menace, certains critiques ont fait valoir que l'analyse du tribunal a sous-estimé l'intégration des mondes numérique et réel en traitant une foule de comportements de M. Corby et d'événements connexes comme des faits isolés (Bailey et Mathen, 2019). Selon le tribunal, les publications étaient bénignes. Si « certaines des images avaient une signification ou une portée particulière pour [la plaignante] », elles ne lui étaient pas destinées et ont été publiées « pour que tout utilisateur de Facebook puisse les voir » [traduction libre] (BCPC, 2012).

Selon Bailey et Mathen (2019), le droit criminel ne devrait pas être l'unique, ni même la principale, réponse à la violence contre les femmes et les filles facilitée par la technologie. Dans de nombreux cas, les victimes et les survivantes ont des raisons fondées de choisir d'autres options (section 3.1.2). L'élimination de la violence facilitée par la technologie nécessite des ressources qui dépassent « la capacité d'un système de justice pénale réactif et punitif » [traduction] (Bailey et Mathen, 2019).

5.1.3 Les délits civils en common law

Le droit de la responsabilité délictuelle est un domaine du droit privé qui vise à indemniser les personnes lésées par les actes répréhensibles d'autrui. Les délits ne doivent pas être confondus avec les crimes, qui sont des infractions contre l'État ou l'ordre public, poursuivies et punies par l'État (Beswick, 2022). Un délit peut être défini comme « un acte ou une omission qui cause une blessure ou un préjudice à une autre personne et qui constitue une faute civile pour laquelle les tribunaux imposent une obligation » [traduction libre] (LII, s.d.). Les poursuites relevant du droit de la responsabilité délictuelle sont généralement intentées par des parties privées qui cherchent à obtenir réparation.

Alors que la responsabilité criminelle a pour but de faire respecter la justice publique, le droit de la responsabilité délictuelle a pour fonction principale d'indemniser la victime. Ainsi, le principal recours du droit de la responsabilité délictuelle est l'attribution de dommages-intérêts au plaignant (LII, s.d.). En plus de dédommager la victime, il peut « servir de médiateur pour le comportement social et protéger les droits fondamentaux » [traduction libre] (Laidlaw, 2021a). Dans le contexte des technologies perturbatrices, le droit de la responsabilité délictuelle peut reconnaître les risques pour la vie privée et définir ce qu'est un comportement raisonnable (Laidlaw, 2021a). Bien que le droit de la responsabilité délictuelle soit principalement établi par les juges, une partie est décrite dans les lois (Laidlaw, 2021a; Beswick, 2022).

Certaines des activités préjudiciables examinées dans le présent rapport peuvent être punissables en vertu du droit criminel ou du droit de la responsabilité délictuelle. Par exemple, la diffusion non consensuelle d'images intimes est un délit civil aussi bien qu'une infraction criminelle. En outre, certains juristes avancent que « menacer de distribuer une image intime d'une personne afin de la contraindre à faire quelque chose constitue le délit d'intimidation » [traduction libre] (Dunn et Petricone-Westwood, 2018). Bien que la réparation soit prévue par le droit criminel et le droit de la responsabilité délictuelle, l'accès à la justice pour les victimes et les survivantes de crimes cyberfacilités demeure problématique. En effet, le système de justice pénale du Canada connaît d'importants arriérés et

retards (LCJC, 2017). De même, les procès devant les tribunaux civils sont onéreux et donnent rarement les résultats escomptés pour les victimes et les survivantes (Laidlaw, 2021a). Dans de nombreux cas, les victimes ne connaissent pas l'identité des abuseurs qui se cachent derrière des comptes d'utilisateurs anonymes. Parfois, l'anonymat des auteurs présumés d'abus empêche les plaignantes d'intenter une action en responsabilité délictuelle (Balkin, 2009; Citron, 2009; Zimmer, 2022). Par conséquent, bien que les recours publics et privés soient tous deux prévus par la loi, leur efficacité est limitée, au mieux.

Les possibilités de protéger la vie privée par l'entremise du droit de la responsabilité délictuelle varient selon la province

La Colombie-Britannique, la Saskatchewan, le Manitoba et Terre-Neuve-et-Labrador ont introduit des causes (motifs) d'action civiles en responsabilité délictuelle pour les atteintes à la vie privée (Laidlaw, 2021a). Plusieurs provinces — l'Alberta, la Saskatchewan, le Manitoba, la Nouvelle-Écosse, Terre-Neuve-et-Labrador, le Nouveau-Brunswick et l'Île-du-Prince-Édouard — ont également adopté des lois spécifiques créant le délit de diffusion non consensuelle d'images intimes (Gouv. de la N.-É., 2022). Bien que la transmission non consensuelle d'images intimes soit une infraction criminelle, le droit de la responsabilité délictuelle cherche à offrir aux victimes un mécanisme plus efficace garantissant le retrait du contenu d'Internet ou la désindexation des résultats des moteurs de recherche (Zimmer, 2022).

Dans l'affaire *Jones c. Tsige*, la Cour d'appel de l'Ontario a reconnu un délit de common law d'intrusion dans l'intimité[10]. Dans cette affaire, M^me^ Jones (la demanderesse) a intenté une action en responsabilité délictuelle contre M^me^ Tsige (la défenderesse) lorsqu'elle a découvert que cette dernière avait accédé à ses renseignements bancaires personnels 174 fois sur une période de 4 ans. Bien que M^me^ Tsige n'ait jamais utilisé ces renseignements et ne les ait jamais divulgués à des tiers, la Cour d'appel de l'Ontario a jugé que la défenderesse avait intentionnellement porté atteinte à la vie privée de la demanderesse (ONCA, 2012).

Ce délit a aussi été reconnu en Nouvelle-Écosse (Laidlaw, 2021a), ce qui a ouvert la voie à la reconnaissance judiciaire d'un autre délit concernant la vie privée appelé « divulgation publique de faits privés » [traduction libre] en Ontario et en Alberta (Mizrahi, 2018; Thiessen *et al.*, 2021). Ce délit civil prévoit que « [quiconque] fait connaître publiquement un élément concernant la vie privée d'autrui est susceptible d'être tenu responsable envers autrui pour atteinte à la vie privée d'autrui, si l'élément rendu public ou l'acte de publication (a) serait hautement préjudiciable à une personne raisonnable et (b) n'est pas une préoccupation

10 Ce délit inclut « les intrusions physiques dans des lieux privés ainsi que l'écoute ou l'observation, avec ou sans aide mécanique, des affaires privées de la demanderesse » [traduction libre] (ONCA, 2012).

légitime du public » [traduction libre] (ONSC, 2016). À titre de réparation, il peut être ordonné au défendeur de tout mettre en œuvre pour retourner toutes les images du demandeur, de retirer toute image publiée en ligne et de payer des dommages-intérêts généraux, des dommages-intérêts punitifs et des dommages-intérêts aggravés pour abus de confiance et détresse mentale (ONSC, 2016).

Dans l'affaire *Caplan c. Atas*, la Cour supérieure de justice de l'Ontario a reconnu que les délits existants ne permettaient pas de traiter correctement l'intention distinctive et malveillante des auteurs de harcèlement sur Internet, ni de dédommager les victimes et les survivants; elle a donc reconnu un délit de harcèlement sur Internet (ONSC, 2021). En particulier, la Cour a estimé que l'auteur de l'infraction dans cette affaire avait fait plus que porter atteinte à la réputation et visait plutôt à susciter « la peur, l'anxiété et la misère » [traduction libre] par des publications sur Internet systématiques et en série de matériel diffamatoire (Koczerginski, 2021). La Cour a accordé une injonction permanente contre M^{me} Atas, a conféré aux demandeurs le titre de propriété des messages diffamatoires et a indiqué qu'elle rendrait des ordonnances accessoires pour permettre aux demandeurs de retirer le contenu (ONSC, 2021).

De plus, dans l'affaire *Yenovkian c. Gulian*, la Cour supérieure de justice de l'Ontario a reconnu le délit de « publicité représentant une personne sous un faux jour » [traduction libre] (ONSC, 2019). Contrairement au droit existant en matière de diffamation, ce délit concernant la vie privée protège le droit d'un individu à déterminer son image publique. Ce délit est « établi lorsqu'une personne est dépeinte sous un faux jour en public, que la fausse représentation serait hautement préjudiciable à une personne raisonnable et que l'auteur du délit savait que la représentation était fausse » [traduction libre] (Cumbo-Steinmetz *et al.*, 2020). Dans cette affaire, le défendeur s'est engagé dans une campagne de cyberintimidation abusive contre la demanderesse et sa famille en diffusant sur Internet des documents contenant de fausses informations (ONSC, 2019). La Cour a estimé que le défendeur avait dépeint la demanderesse sous un faux jour et que son comportement avait causé un préjudice grave, notamment une « maladie visible et prouvable » [traduction libre] et des inquiétudes quant à la façon dont des étrangers pourraient maltraiter la demanderesse sur la base des informations diffusées en ligne (ONSC, 2019). Le tribunal a condamné le défendeur à payer 300 000 dollars en dommages-intérêts.

Les délits qui existent au Canada reposent souvent sur une notion dépassée de ce qu'est la vie privée

Les délits mentionnés précédemment ont toutefois une portée limitée (Mizrahi, 2018; Laidlaw, 2021a). Par exemple, ils sont fondés sur une notion dépassée selon laquelle la vie privée est « ce qui se passe lorsque nous sommes dans l'intimité ou

seuls, que la protection de la vie privée ne protège que les comportements déviants ou intimes et que le contexte n'a pas d'importance » [traduction libre] (Laidlaw, 2021a). À l'ère du numérique, le droit à la vie privée est presque toujours en jeu, car les gens doivent constamment participer à l'économie fondée sur les données. Pourtant, selon les circonstances, certaines atteintes à la vie privée numérique, comme les hypertrucages, ainsi que l'amplification par les moteurs de recherche, « ne pourraient probablement pas faire l'objet d'une poursuite pour délit concernant la vie privée » [traduction libre] (Laidlaw, 2021a). Les cadres dépassés du droit de la responsabilité délictuelle en matière de vie privée ne tiennent donc pas nécessairement compte des préjudices contemporains dans le monde interconnecté.

Les juristes et les praticiens avancent toutefois que certains délits supplémentaires pourraient être applicables aux crimes et préjudices cyberfacilités (Dunn et Petricone-Westwood, 2018). Par exemple, la diffusion non consensuelle d'images intimes peut mener à un délit d'appropriation de la personnalité, d'abus de confiance, de manquement à une obligation fiduciaire, etc. Cependant, le potentiel des délits suggérés par les juristes pour protéger la vie privée constitue un domaine encore nouveau du droit civil, car la plupart des cas signalés de diffusion non consensuelle d'images intimes ont fait l'objet de poursuites en vertu du droit criminel (Dunn et Petricone-Westwood, 2018). D'autres études, ainsi que des évaluations de procès, peuvent être nécessaires pour justifier l'utilité de l'application de ces délits aux préjudices cyberfacilités.

5.1.4 Législation pertinente en matière de protection de la vie privée

La Loi sur la *protection des renseignements personnels et les documents électroniques* (LPRPDE) exige que les organisations du secteur privé obtiennent le consentement avant de recueillir, d'utiliser ou de communiquer des renseignements personnels

Au Canada, lorsque des individus subissent un préjudice touchant la vie privée, ils peuvent se tourner vers la loi fédérale dans l'espoir de résoudre le problème. La loi fédérale canadienne sur la protection des renseignements personnels, la LPRPDE, s'applique aux organisations du secteur privé qui « recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales » (CPVP, 2019c; Schwartz *et al.*, 2021). En vertu de la LPRPDE, les renseignements personnels comprennent toute information factuelle ou subjective sur une personne identifiable, notamment son nom, son origine ethnique, son âge, un numéro d'identification, son revenu, ses opinions, ses évaluations, ses dossiers d'employés et ses dossiers financiers et médicaux (CPVC, 2019c). La LPRPDE interdit aux organisations de recueillir, de communiquer ou

d'utiliser des renseignements personnels sans le consentement de l'intéressé (sauf dans certaines circonstances) et établit un régime de signalement des atteintes à la vie privée (The eQuality Project, s.d.) (encadré 5.2).

Encadré 5.2 Violations de données et LPRPDE

L'une des raisons pour lesquelles les particuliers peuvent se tourner vers la LPRPDE est de déterminer les recours dont ils disposent en cas de violation de la confidentialité des données. Toute entreprise tombant sous le coup de la loi doit divulguer les atteintes à la vie privée au Commissariat à la protection de la vie privée du Canada (CPVP) et à la personne concernée. Les atteintes doivent être signalées lorsqu'il existe un « risque réel de préjudice grave pour un individu » (GC, 2000a). Le paragraphe 10.1(7) de la LPRPDE stipule que le « préjudice grave » comprend, entre autres, l'humiliation, le dommage à la réputation ou aux relations et le vol d'identité. En vertu du paragraphe 10.1(4), l'avis à la personne concernée doit contenir « suffisamment d'information pour permettre à l'intéressé de comprendre l'importance, pour lui, de l'atteinte et de prendre, si cela est possible, des mesures pour réduire le risque de préjudice qui pourrait en résulter ou pour atténuer un tel préjudice » (GC, 2000a).

Le respect de la LPRPDE est contrôlé par le CPVP, qui peut, de sa propre initiative, examiner des plaintes déposées par des individus à propos des pratiques de gestion de l'information d'entreprises privées dans toute province qui n'a pas adopté une loi sur la protection des renseignements personnels essentiellement similaire (CPVP, 2017a; Mizrahi, 2018). En juin 2022, la Colombie-Britannique, l'Alberta et le Québec avaient adopté des lois sur la protection des renseignements personnels « essentiellement similaires » à la LPRPDE, ce qui signifie que leurs propres lois provinciales s'appliquent souvent en lieu et place de la LPRPDE (CPVP, 2016a; Schwartz *et al.*, 2021). Le CPVP examine fréquemment des plaintes concernant l'usurpation d'identité et la diffusion non consensuelle d'images intimes (CPVP, 2016b). À ce jour, il s'est penché sur des cas concernant le fonctionnement de sites et services de rencontres en ligne, de sites Web qui réaffichent des décisions de tribunaux et de cours de justice et de nombreux sites Web dits de *vengeance* et de dénigrement, entre autres (CPVC, 2016b).

La LPRPDE est restreinte par des difficultés d'application

Comme nous le notons au chapitre 2, la LPRPDE vise à réglementer la relation entre les entreprises et les individus, plutôt qu'à protéger la vie privée en tant que droit de la personne[11]. Bien qu'elle cherche à assurer une protection adéquate des renseignements personnels des personnes identifiables, l'application réelle de la LPRPDE à certains cyberméfaits et crimes cyberfacilités peut être floue. Par exemple, les vidéos hypertruquées peuvent ne pas enfreindre la loi sur la protection des renseignements personnels parce qu'elles n'exposent pas la vie réelle des victimes et des survivants (McMillan, 2018). De plus, si un individu utilise les vidéos personnelles de quelqu'un pour produire une vidéo hypertruquée à des fins non commerciales, la LPRPDE ne s'appliquera pas (CPVP, 2017b). Néanmoins, lorsqu'elles créent une fausse impression de la vie privée d'une personne, les vidéos hypertruquées peuvent causer de réels préjudices, comme lorsqu'une vraie vidéo d'une activité similaire est partagée sans consentement (chapitre 3).

L'un des plus gros défis auxquels le CPVP est confronté lorsqu'il s'agit de protéger la réputation en ligne est d'affirmer sa compétence sur les sites Web situés hors Canada. Dans certains cas, ces sites peuvent ne pas être assujettis à la LPRPDE parce que leur ou leurs exploitants n'ont pas de lien réel et substantiel avec le Canada (CPVP, 2016b). De plus, pour que la LPRPDE s'applique, il faut qu'un site Web mène des activités commerciales; dans certains cas, des renseignements personnels sont affichés sans consentement sur des sites créés pour un usage personnel (CPVP, 2016b). Si le CPVP est compétent, il peut demander à une organisation (p. ex. une plateforme de médias sociaux) de retirer du contenu (The eQuality Project, s.d.), mais pour faire respecter cette demande, il faut engager une procédure devant la Cour fédérale (CPVP, 2016a).

Bien que le CPVP soit mandaté pour examiner des plaintes, il n'est pas habilité à accorder des compensations. La loi offre aux individus la possibilité de porter l'affaire devant la Cour fédérale, mais « il est extrêmement rare que des dommages-intérêts soient accordés, et seulement dans les situations les plus flagrantes » [traduction libre] (Mackey, 2012). En outre, comme dans le cas du droit de la responsabilité délictuelle, les particuliers ont peu de possibilités d'invoquer des réparations dans le cadre du régime fédéral de protection de la vie privée en raison de la difficulté d'intenter des poursuites privées contre les contrevenants (Scassa, 2018).

11 Le commissaire à la protection de la vie privée du Canada a toutefois fait valoir que la LPRPDE devrait aborder la protection des renseignements personnels sous l'angle des droits de la personne (CPVP, 2021b).

L'absence de principes communs inscrits dans les lois sur la protection de la vie privée dans les secteurs public et privé nuit à l'efficacité de la LPRPDE

Les partenariats public-privé faisant appel à des technologies numériques sont source de risques pour la vie privée (Therrien, 2021b). Ceci était particulièrement vrai au moment de la COVID19, durant laquelle plusieurs initiatives gouvernementales relatives à la pandémie incluaient des partenariats avec le secteur privé. Les institutions gouvernementales n'étaient pas tenues de garantir un consentement significatif à ces initiatives, puisque l'autorité légale était basée sur le consentement obtenu par une organisation privée (Therrien, 2021b). Par conséquent, il y avait un risque que le secteur public mette en œuvre une solution technologique (p. ex. des platesformes de télémédecine ou d'apprentissage en ligne) permettant à un partenaire privé d'utiliser des renseignements personnels, même si ces renseignements avaient été recueillis pour des questions privées concernant la santé (CPVP, 2020a). Une enquête du CPVP sur les mesures prises par Statistique Canada soulève des craintes similaires : ce dernier organisme a commencé à collecter des renseignements détaillés sur le dossier de crédit d'individus résidant au Canada auprès d'entreprises privées et prévoyait recueillir d'autres données sur les transactions financières et le solde de comptes. Ces initiatives portaient atteinte à la vie privée, mais, en partie à cause de l'inadéquation des lois fédérales, l'enquête du CPVP n'a pas révélé d'infraction légale (Therrien, 2021b).

5.1.5 Protection de la vie privée au Québec

Alors que la common law régit les relations entre les personnes dans toutes les autres provinces, c'est le *Code* civil qui s'applique au Québec. Cette différence essentielle a des conséquences sur le régime juridique concernant les contrats, les délits et la propriété (Beaulac et Gaudreault-DesBiens, 2017), entre autres. De plus, l'article 5 de la *Charte des droits et libertés de la personne* du Québec reconnaît la vie privée comme un droit de la personne et garantit le droit à la vie privée en permettant aux personnes concernées d'engager des poursuites (Gouv. du QC, 1976; Stoddart, 2007). En 1982, le Québec a adopté la première loi sur la protection des renseignements personnels dans le secteur public (Gouv. du QC, 1982) et, en 1994, il est devenu la première province du Canada à adopter une loi sur la protection de ces mêmes renseignements dans le secteur privé (Delwaide et Aylwin, 2005). Toutes ces lois s'accompagnent d'une jurisprudence sur les questions de vie privée (Delwaide et Aylwin, 2005).

Un chapitre du *Code civil* du Québec est consacré à la vie privée (c.-à-d. les articles 35 à 41). L'article 35 établit le droit de toute personne au respect de sa réputation et de sa vie privée, l'article 36 fournit une liste non exhaustive des

actes qui peuvent porter atteinte à la vie privée d'une personne et l'article 37 exige que « toute personne qui constitue un dossier sur une autre personne » ait un « intérêt sérieux et légitime à le faire » (Gouv. du QC, 1991). Une atteinte au droit à la vie privée peut donner lieu à une compensation sous forme de dommages-intérêts monétaires, non monétaires ou punitifs (Norton Rose Fulbright, 2012).

Les dispositions du *Code civil* relatives à la vie privée s'appliquent aux espaces numériques (Schwartz *et al.*, 2021). Par exemple, plusieurs poursuites civiles ont été engagées devant les tribunaux québécois dans des circonstances similaires au partage non consensuel d'images intimes. Les réparations accordées dans ces affaires étaient fondées, entre autres, sur les dispositions relatives à la protection de la vie privée de la Charte provinciale et du *Code civil*. Cependant, les dommages-intérêts ont été difficiles à établir, les sommes accordées ont été très faibles et l'effet dissuasif a été minime (Boutin-Clermont, 2014).

Certains concepts contenus dans le *Code civil* — comme le respect de la réputation et le droit de la personnalité — ne sont pas utilisés dans la common law à l'extérieur du Québec. Bien que les délits civils en matière de vie privée adoptés en Colombie-Britannique, en Saskatchewan, au Manitoba et à Terre-Neuve-et-Labrador visent à améliorer la protection de la vie privée, ils semblent s'appliquer dans des circonstances limitées; la plupart des provinces n'ont pas introduit la législation ou les concepts connexes de protection de la vie privée qui existent dans le droit civil du Québec (Stoddart, 2004).

La loi québécoise sur la protection de la vie privée dans le secteur privé a une portée plus large et des mesures d'application plus strictes que la LPRPDE

Le Québec a entrepris une réforme complète de son régime de protection de la vie privée dans le secteur privé, dans le but de l'adapter aux réalités d'aujourd'hui. En 2021, l'Assemblée nationale du Québec a adopté le projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25) (Gouv. du QC, 2021). Bon nombre des obligations contenues dans ce projet de loi coïncident avec les dispositions relatives à la protection de la vie privée de la LPRPDE ou avec les recommandations du CPVP. Cependant, les obligations de la loi en matière de protection de la vie privée contiennent des mesures d'application strictes, plutôt que de fortes recommandations, comme c'est le cas dans la LPRPDE (McMillan, 2021). Elles créent un droit de poursuite privé pour les individus en cas d'atteinte illégale à leurs droits prévus par la loi et aux dispositions du *Code* civil relatives à la vie privée (CPVP, 2020b).

En vertu de la Loi 25, les entreprises[12] doivent signaler les incidents de confidentialité, faire des efforts raisonnables pour réduire le risque de préjudice et prévenir les incidents futurs (Gouv. du QC, 2021). Un *incident de confidentialité* « s'entend de l'utilisation ou de la communication de renseignements personnels ou de leur accès non autorisés par la Loi, ainsi que de la perte de tels renseignements ou de tout manquement à leur protection» (McMillan, 2021). Cette définition diffère de ce que l'on retrouve dans les autres lois canadiennes sur la protection de la vie privée en ce qu'elle traite l'utilisation non autorisée de renseignements personnels comme un incident de confidentialité. Par conséquent, la Loi 25 « va au-delà des exigences en matière de notification de la violation de la confidentialité des données à caractère personnel des autres lois canadiennes » (McMillan, 2021) et a pour effet de créer potentiellement un régime de notification à deux vitesses : une pour les résidents du Québec et une autre pour les résidents des autres parties du pays.

Dans les cas où un *incident de confidentialité* présente un risque de préjudice sérieux, une organisation doit aviser la Commission d'accès à l'information du Québec et toute personne dont les renseignements personnels sont touchés par l'incident (Gouv. du QC, 2021). Ce seuil de notification est similaire au seuil de notification d'un « risque réel de préjudice grave » de la LPRPDE (McMillan, 2021). La Loi 25 ne fournit pas de définition ni d'exemple de ce qu'est un *risque de préjudice grave*. Toutefois, elle fixe plusieurs critères que les organisations doivent prendre en compte pour déterminer la gravité d'un tel risque : la sensibilité des renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables (BLG, 2021). Bien que les critères d'évaluation de la Loi 25 semblent être similaires à ceux de la LPRPDE, la Commission peut interpréter les exigences de notification différemment du CPVP (BLG, 2021). Par conséquent, les résidents du Québec peuvent être soumis à des normes de notification différentes selon la loi — la LPRPDE ou la nouvelle loi découlant de la Loi 25 — qui régit l'organisation signalant l'incident.

5.1.6 Droit relatif à la diffamation

Au Canada, le droit relatif à la diffamation protège la réputation en imposant des limites à la liberté d'expression, dans les cas où de fausses déclarations portent atteinte à la réputation. Il établit ainsi un équilibre entre deux valeurs canadiennes : la valeur quasi constitutionnelle de la protection de la réputation (CSC, 1995; CDO, 2020) et la protection constitutionnelle de la liberté d'expression, reconnue dans la *Charte canadienne des droits et libertés* (GC, 1982). Les principes

12 La définition d'*entreprise* regroupe un large éventail d'activités. Toutefois, lorsqu'il s'agit de déterminer si une organisation est une entreprise, ou si une personne exploite une entreprise, les tribunaux considèrent l'activité principale, plutôt que les activités accessoires (Delwaide et Aylwin, 2005).

concernant la diffamation au Canada sont principalement dictés par la common law, complétée par la législation (ce qui entraîne des variations au pays) (CDO, 2020). Au Québec, la diffamation relève des dispositions du *Code civil* relatives à la responsabilité civile (CSC, 2011). Comme les valeurs de liberté d'expression et de protection de la réputation sont influencées par le contexte et les normes sociales, le droit relatif à la diffamation dépend de la société et de la culture dans lesquelles il s'applique. Dans la plupart des cas, il évolue au cas par cas, en réponse à des plaintes particulières déposées devant les tribunaux.

Le droit relatif à la diffamation a été lent à s'adapter à la prolifération sur Internet

Bien que le droit relatif à la diffamation ne soit pas spécifique aux activités en ligne, selon la Commission du droit de l'Ontario (CDO) (2020), « Internet est à présent l'espace où on signale la plupart des actes diffamatoires, si ce n'est leur totalité » et certains des actes préjudiciables examinés au chapitre 3 peuvent contenir de la diffamation. Par exemple, certaines vidéos hypertruquées peuvent créer de fausses affirmations sur les faits concernant une personne et entraîner une perte de réputation (McMillan, 2018). Les victimes et les survivants de diffamation peuvent avoir droit à des dommages-intérêts et à une mesure injonctive pour empêcher la diffusion de documents diffamatoires. Toutefois, lorsqu'une vidéo contient un avertissement indiquant qu'elle est truquée, l'action en diffamation peut échouer. La nature mondiale des activités sur Internet peut également créer des difficultés pour les affaires de diffamation au Canada, car les tribunaux canadiens peuvent ne pas être compétents si l'éditeur de la vidéo est situé à l'étranger (McMillan, 2018). Ainsi, les personnes ciblées par ces vidéos disposent, en pratique, d'un recours juridique limité lorsqu'une vidéo est qualifiée de « fausse » ou lorsque les éditeurs agissent à l'extérieur de la juridiction d'un tribunal canadien.

La prolifération du contenu numérique a entraîné d'importants changements dans l'étendue et la propagation de la diffamation. Ce qui était autrefois un problème local est maintenant de plus en plus un problème transnational, car le contenu diffamatoire peut être rendu public dans le monde entier (CDO, 2020). Autrefois, les défendeurs dans les cas de diffamation étaient des éditeurs ou des organes de presse qui produisaient des journaux, des livres ou des émissions de télévision et de radio. Aujourd'hui, à l'ère de l'Internet, ce sont souvent des éditeurs individuels qui publient des documents en ligne. La CDO (2020) note que le droit a eu « de la difficulté à s'adapter » à ces nouveaux types d'affaires, puisqu'il s'est inscrit « essentiellement dans les limites de ce paradigme traditionnel ».

À la lumière de ces défis, des appels à la mise à jour du droit relatif à la diffamation ont été lancés (Laidlaw et Young, 2017; CDO, 2020). En ce qui a trait à la responsabilité des intermédiaires pour le contenu diffamatoire publié par des

tiers, Laidlaw et Young (2017) affirment que « la loi est complexe et confuse », ce qui mène à un cadre de gouvernance « mal adapté pour traiter la question de la responsabilité des intermédiaires sur Internet en matière de diffamation » [traduction libre]. La doctrine conduit parfois à ce que des intermédiaires soient considérés comme des éditeurs dans des cas où « beaucoup ne penseraient pas que leur comportement est suffisamment répréhensible pour justifier qu'ils soient tenus responsables » [traduction libre]. Étant donné l'incertitude et de la confusion, certains juristes sont d'avis que les intermédiaires ne devraient pas être tenus responsables des actes illicites de tiers et qu'ils devraient plutôt disposer de procédures pour traiter les plaintes en diffamation et retirer le contenu prétendument diffamatoire dans des circonstances strictes. Ces propositions visent à trouver un équilibre entre la liberté d'expression et la protection de la réputation (Laidlaw et Young, 2017).

5.1.7 Lois et règlements sur le blanchiment d'argent et rôle du CANAFE

Les lois et règlements sur le blanchiment d'argent offrent d'autres voies juridiques pour assurer la sécurité des personnes au Canada (GC, 2021e). Comme nous le mentionnons à la section 4.1, le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) a été fondé en 2000 pour garantir la conformité du Canada aux normes internationales de lutte contre le blanchiment d'argent (CANAFE, 2021a). Il est régi par la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* et ses règlements, il applique les dispositions de la *Loi antiterroriste* et sert de « centre d'échange, recevant, analysant et communiquant des renseignements financiers à propos de soupçons de blanchiment d'argent, de financement d'activités terroristes et de menaces à la sécurité du Canada » [traduction libre] (Pyrik, 2021).

Le CANAFE n'a pas de pouvoirs d'enquête et des forces de l'ordre, et il est détaché des organismes d'application de la loi

Le CANAFE relève du ministère des Finances. Il est indépendant des forces de l'ordre canadiennes et ne dispose pas de pouvoirs d'enquête indépendants. L'alinéa 40(a) de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* stipule que le CANAFE « est autonome et indépendant de tout organisme chargé de l'application de la loi et des autres entités » (GC, 2000b). Il est toutefois autorisé à divulguer des renseignements désignés, bien que ces renseignements ne comprennent pas « de renseignements de source ouverte [...], une théorie du crime ou la justification écrite interne de la divulgation » [traduction libre] (Pyrik, 2021). Par conséquent, les destinataires doivent reproduire les actions du CANAFE ou utiliser une ordonnance de communication pour accéder aux renseignements.

Le CANAFE possède un mandat plus limité et moins de possibilités de coopération que les organismes similaires d'autres pays (FINA, 2018). Par exemple, aux États-Unis, le Financial Crimes Enforcement Network (FinCEN) relève également de l'organisme responsable des finances fédérales (le département du Trésor), mais la *USA Patriot Act* l'autorise à exercer certaines activités que le CANAFE ne peut pas entreprendre (p. ex. ordonner aux institutions financières de fournir des renseignements sur des personnes ou des entités soupçonnées d'activités criminelles à la demande des forces de l'ordre nationales et de certains organismes étrangers) (FINA, 2018). De son côté, la Financial Intelligence Unit du Royaume-Uni relève du Home Office, qui est responsable de la sécurité publique et de l'immigration, et non du HM Treasury (ministère des Finances).
Le fait que le CANAFE relève du ministère des Finances présente à la fois des avantages et des inconvénients; cette structure organisationnelle renforce les liens entre le CANAFE et les institutions financières canadiennes, mais nuit à la coopération entre le CANAFE et les forces de l'ordre (FINA, 2018; Pyrik, 2021).

Le CANAFE continue de se heurter à des difficultés dans la surveillance des transactions effectuées dans le cadre d'échanges décentralisés entre pairs

Les monnaies numériques, telles que le Bitcoin ou l'Ether, peuvent faciliter les transactions pseudonymes ou anonymes sans surveillance ou intervention d'un tiers (section 4.1.2); cette propriété a rendu les cryptomonnaies intéressantes pour certains acteurs criminels, tels que ceux qui mènent des opérations au moyen de rançongiciels. Devant cette situation, le gouvernement du Canada a modifié le régime juridique de la prévention du blanchiment d'argent et du financement du terrorisme. Tout d'abord, en 2020, un règlement a défini la *monnaie virtuelle* de la façon suivante :

> *(a) représentation numérique de valeur pouvant être utilisée comme mode de paiement ou à titre de placement, qui n'est pas une monnaie fiduciaire et qui peut être facilement échangée contre des fonds ou contre une autre monnaie virtuelle qui peut être facilement échangée contre des fonds;*
>
> *(b) [une] clé privée d'un système de chiffrement permettant à une personne ou entité d'avoir accès à une telle représentation numérique de valeur.*
>
> GC (2020b)

Deuxièmement, la définition d'*entreprise de services monétaires* (ESM) a été modifiée pour inclure toute personne « faisant le commerce de monnaies virtuelles » [traduction libre] (Pyrik, 2021). Une telle personne doit s'inscrire en tant qu'ESM auprès du CANAFE et se conformer aux exigences de déclaration, de tenue de dossiers, de connaissance du client et de conformité (Bennett Jones, 2021). Troisièmement, les obligations des autres entités déclarantes (telles que les

banques, les caisses populaires, les compagnies d'assurance et les casinos) s'étendent aux transactions en monnaie virtuelle (Bennett Jones, 2021). Toutes ces modifications devraient permettre au CANAFE de surveiller les mouvements et l'utilisation des monnaies numériques et, à ce titre, de leur ôter au moins une partie de leur pseudonymat ou de leur anonymat.

En outre, fin 2020, le CANAFE a publié des indicateurs de blanchiment d'argent et de financement du terrorisme au moyen de transactions en monnaie virtuelle. Ces indicateurs ont été élaborés après une analyse des affaires de blanchiment et de terrorisme, des déclarations de transactions suspectes, des commentaires d'entités déclarantes et des documents publiés par les organismes internationaux chargés de l'application de la loi (Badour *et al.*, 2020). En 2021, le CANAFE a publié une version actualisée de ces indicateurs (CANAFE, 2021c).

Cependant, malgré les efforts déployés pour modifier les règles en vigueur, le CANAFE continue de faire face à des défis en matière de surveillance des transactions effectuées dans des plateformes d'échange décentralisées (DEX) de pair à pair, qui ne nécessitent pas de contrôleur ou de bailleur de fonds tiers (Keatinge *et al.*, 2018; Dolny, 2021). L'origine des transferts de gros volumes et fréquents de monnaies confidentielles entre individus anonymes est, à l'heure actuelle, très difficile à examiner, et les directives mentionnées précédemment ne règlent pas le problème (Dolny, 2021). En avril 2021, 122 milliards de dollars US de transactions ont eu lieu sur ces platesformes, contre 1 milliard de dollars US un an plus tôt (Osipovich, 2021); la valeur moyenne du Bitcoin, l'une des principales cryptomonnaies, a augmenté de 300 % entre janvier et décembre 2020 (DeMatteo, 2022). Cependant, au cours du premier semestre 2022, elle a diminué de plus de 50 % par rapport à son sommet historique, pour atteindre un montant inférieur à celui de décembre 2020 (Gailey et Haar, 2022).

5.1.8 Loi canadienne antipourriel

La fraude, la cyberintimidation et le cyberharcèlement peuvent s'effectuer sur des sites de commerce électronique ou par le biais d'un marketing trompeur, de courriels promotionnels, de messages texte ou de messages instantanés. La *Loi canadienne antipourriel* (LCAP) joue un rôle important dans la prévention des crimes et des méfaits cyberfacilités en réglementant les activités courantes des entreprises, comme l'envoi de courriels aux clients, l'exploitation du site Web de l'entreprise et le téléchargement d'applications mobiles (Olser, s.d.). Selon le GC (2021f), dans le cadre d'une activité commerciale, la LCAP interdit, entre autres, le pollupostage, le marketing trompeur, l'installation de logiciels malveillants et de logiciels espions, le piratage et la collecte d'adresses. Les sanctions pour certaines infractions à la LCAP peuvent atteindre 1 million de dollars pour les particuliers et 10 millions de dollars pour les entreprises (GC, 2019c). Bien que la LCAP crée un

régime de gouvernance complet pour lutter contre tout un éventail d'actes préjudiciables, sa mise en œuvre fructueuse nécessite des ressources importantes, la sensibilisation et la participation de la population, la coordination avec les forces de l'ordre et la clarification de certaines ambiguïtés juridiques.

Les dispositions de la LCAP sur la responsabilité des intermédiaires sont ambiguës

La LCAP « a créé une infraction de responsabilité stricte pour les intermédiaires qui permettent l'envoi de messages électroniques non sollicités ou similaires ou en bénéficient financièrement, notamment les courtiers en publicité, les spécialistes du marketing électronique, les développeurs et les fournisseurs de paiement » [traduction libre] (Laidlaw, 2019). Par exemple, les intermédiaires pourraient être tenus responsables des manquements à la LCAP commis par des tiers. Des inquiétudes ont été soulevées au sujet des dispositions relatives à la responsabilité, qui pourraient s'appliquer « même si l'intermédiaire n'avait pas l'intention de contribuer à une infraction à la LCAP ou n'était pas conscient que ses activités permettaient ou facilitaient des infractions » [traduction libre] (Kratz, 2019). Ce cadre réglementaire a été décrit comme « complexe, lourd et ambigu » [traduction libre] (Kratz, 2018).

Les exigences concernant les logiciels malveillants de la LCAP ont reçu un large soutien

Contrairement aux dispositions sur la responsabilité des intermédiaires, les exigences de la LCAP relatives à la lutte contre les logiciels malveillants ont reçu un large soutien (Kratz, 2020). L'article 8(1) de la Loi prévoit qu'il est « interdit, dans le cadre d'activités commerciales, d'installer ou de faire installer un programme d'ordinateur dans l'ordinateur d'une autre personne [...] sauf si la personne qui accomplit l'acte en question [...] le fait avec le consentement exprès du propriétaire ou de l'utilisateur de l'ordinateur » (GC, 2010). Selon le comité d'experts, cela signifie que la LCAP permet de prendre des mesures contre les entreprises qui fournissent des logiciels espions ou malveillants pour le suivi et la surveillance des appareils personnels de son conjoint. Toutefois, l'efficacité réelle du recours à la LCAP dans ces situations reste à voir, en attendant qu'un certain nombre d'enquêtes aient été menées et que des mesures aient été prises.

En outre, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) prévoit d'exiger des fournisseurs d'accès Internet (FAI) qu'ils bloquent les réseaux de zombies (*botnets*) qui acheminent des logiciels malveillants (CRTC, 2022; Solomon, 2022). Un réseau de zombies « est un réseau d'appareils infectés par des logiciels malveillants et contrôlé en groupe à l'insu et sans le consentement de leurs propriétaires, dans un but malveillant » (CRTC, 2022).

Les réseaux de zombies sont utilisés pour faciliter les logiciels malveillants et les pourriels, les attaques par déni de service distribué et les violations de la confidentialité des données et pour donner aux acteurs malveillants un accès illimité aux réseaux. Lorsque les exigences du CRTC entreront en vigueur, les FAI devront bloquer les réseaux de zombies au niveau du réseau (CRTC, 2022; Solomon, 2022).

La LCAP confère au CRTC des pouvoirs d'application de la loi

En vertu de la LCAP, le CRTC peut imposer des sanctions aux personnes et aux entreprises impliquées dans des marchés perturbateurs (encadré 5.3) et délivrer des mandats de retrait à leur endroit. Le cadre en chef de la Conformité et des Enquêtes du CRTC donne des procèsverbaux de violation accompagnés de sanctions lorsqu'il existe « des motifs raisonnables de croire qu'une violation a eu lieu ». Les contrevenants présumés ont alors 30 jours pour payer la sanction ou contester les procès-verbaux et les sanctions. Depuis sa création, le CRTC a donné plus de 1,4 million de dollars de procès-verbaux (GC, 2022c).

Encadré 5.3 Démantèlement par le CRTC de Canadian HeadQuarters

En janvier 2022, le cadre en chef de la Conformité et des Enquêtes du CRTC a imposé des sanctions d'un montant de 300 000 $ à plusieurs personnes au Canada pour leur participation au marché du Web clandestin appelé Canadian HeadQuarters (également connu sous le nom de Canada HQ ou Canadian HQ), qui a finalement été mis hors ligne. Canadian HeadQuarters était l'une des plus grandes places de marché du Web clandestin au monde. Il se spécialisait dans « la vente de biens et de services, y compris des services de pourriels, des trousses d'hameçonnage, des identifiants volés et des accès aux ordinateurs compromis », qui étaient ensuite utilisés pour faciliter les activités malveillantes. L'enquête du CRTC a porté sur plusieurs personnes qui avaient envoyé des courriels imitant des marques célèbres pour accéder à des renseignements sur des comptes bancaires et à des numéros de cartes de crédit.

(GC, 2022c)

5.2 Sélection d'approches réglementaires étrangères

Le Canada n'est pas le seul pays à tenter de contrer l'éventail d'activités criminelles et préjudiciables en ligne rendues possibles ou plus répandues par les TIC. De nombreux pays alliés du Canada ont adopté des lois pour lutter contre ces maux ou travaillent collectivement pour combattre les préjudices cyberfacilités. Dans cette section, le comité d'experts examine certaines lois promulguées et approches réglementaires proposées concernant ces genres de préjudices. Il se penche principalement sur les pays dont la structure sociopolitique est similaire à celle du Canada, qui entretiennent des relations diplomatiques étroites avec le Canada (p. ex. Groupe des cinq) ou qui influencent la réforme du droit national canadien. Le comité souligne également certaines des limites potentielles, ou réelles, de ces lois et règlements, notamment la manière dont elles pourraient sacrifier la liberté d'expression au profit d'une réglementation accrue.

La gouvernance étatique des espaces numériques peut avoir un effet paralysant sur l'exercice des droits des personnes

Ce que l'on appelle *effet paralysant* décrit toute incidence potentielle que la gouvernance étatique de l'environnement numérique — en particulier, les règlements destinés à contrôler les abus en ligne, le discours haineux ou d'autres méfaits en ligne — peut avoir sur les droits des individus. Dans ce contexte, il s'agit de « l'idée que certaines actions réglementaires peuvent "refroidir" les gens ou les dissuader d'exercer leurs droits en ligne et dans d'autres contextes numériques » [traduction libre] (Penney, 2020). Il existe différentes philosophies concernant ces règlements à l'échelle mondiale. Les modèles européens ont tendance à se concentrer sur la prévention du harcèlement en ligne et à donner la priorité à la protection de la dignité et de la réputation des personnes (Penney, 2019a). En revanche, le modèle américain privilégie la liberté d'expression, ou une large immunité qui vise à éviter tout effet dissuasif du législateur sur cette liberté. Cela s'inscrit parfaitement dans la tradition juridique américaine, qui définit la vie privée comme une liberté face à l'interférence de l'État (Penney, 2019a).

Il existe peu de données prouvant un effet important de la loi sur le discours en ligne d'un utilisateur (Kendrick, 2012; Penney, 2017). Cela peut être dû, en partie, au fait qu'il s'agit d'un sujet difficile à étudier ou à quantifier (Penney, 2020). Les données probantes limitées et nouvelles dont on dispose concernent en grande partie l'application de la *Digital Millennium Copyright Act* (DMCA) des États-Unis. En vertu de la DMCA, des systèmes automatisés exploités par des entités privées envoient des avis de retrait aux fournisseurs de services en ligne, qui retirent alors le contenu violant les lois sur le droit d'auteur et en informent l'utilisateur (Penney, 2019b). Des dizaines de millions de ces avis sont envoyés chaque jour, ce qui amène les critiques à penser que la loi a un effet paralysant en

ligne. Une enquête portant sur 500 comptes Blogger de Google et 500 comptes Twitter a fourni les premières données probantes d'un lien entre l'envoi d'ordres de retrait automatisés et l'effet paralysant (Penney, 2019b). Par exemple, 75 % des répondants à l'enquête ont indiqué qu'ils seraient « beaucoup moins susceptibles » ou « un peu moins susceptibles » « de parler ou d'écrire sur certains sujets en ligne » [traduction libre] après avoir reçu un avis personnel en vertu de la DMCA. Le même scénario inciterait 81 % des personnes interrogées à faire plus attention à ce dont elles discutent sur Internet (Penney, 2019b). En outre, l'enquête a révélé un lien entre la DMCA et les craintes en matière de protection de la vie privée. Par exemple, 81 % des personnes interrogées ont indiqué qu'elles seraient plus préoccupées par la protection de la vie privée et prendraient des mesures supplémentaires pour la protéger si elles recevaient un ordre de retrait. Dans l'ensemble, Penney (2019b) a constaté que les inquiétudes relatives à la vie privée sont le plus grand prédicteur de l'effet paralysant.

Cependant, ceux qui s'opposent aux cadres législatifs ou réglementaires en raison de leur potentiel à limiter la liberté d'expression ignorent souvent l'effet paralysant que le harcèlement en ligne a sur les victimes et sur les droits constitutionnels de ces dernières (Penney, 2020). Penney (2020) invoque l'affaire *Crouch c. Snell*, dans laquelle la Cour suprême de la Nouvelle-Écosse a invalidé la loi sur la cybersécurité (*Cyber-Safety Act*) de la province parce qu'elle empiétait sur la liberté d'expression garantie par la *Charte des droits et libertés* (NSSC, 2015). Si la Cour a reconnu que les victimes et les survivants de cyberintimidation devaient avoir accès à la justice, Penney (2020) note qu'elle n'a pas abordé les répercussions de l'abus en ligne sur la liberté d'expression des victimes.

Comme il est décrit à la section 3.1, de plus en plus d'éléments montrent que le harcèlement en ligne a un effet paralysant important sur les cibles en les forçant à quitter les forums et à cesser d'être actives sur Internet (Franks, 2018; Penney, 2020). Franks (2018) affirme qu'« il existe de nombreuses données probantes sur la façon dont le harcèlement étouffe la liberté d'expression, de mobilité et d'association » [traduction libre], ajoutant que cette conséquence a un effet paralysant plus fort, en particulier sur les femmes et les minorités, que celui qu'une mesure gouvernementale pourrait avoir. Certains chercheurs affirment que les lois et les règlements peuvent même libérer la parole des femmes (Citron et Penney, 2019). Par exemple, dans une étude portant sur 1 200 utilisateurs d'Internet aux États-Unis, les répondantes ont indiqué qu'elles seraient plus susceptibles de produire du contenu autogénéré ou d'être actives sur des sites de réseautage social si des lois les protégeaient contre les préjudices en ligne (Citron et Penney, 2019).

La recherche démontre que l'effet paralysant n'implique pas nécessairement l'autocensure. Il façonne plutôt le comportement social en encourageant les gens à parler ou à agir d'une manière conforme aux normes sociales perçues. Penney

(2022) affirme que les juristes ont largement négligé cette dimension de l'effet paralysant, se concentrant plutôt sur la relation entre l'effet paralysant et la liberté de parole et d'expression.

Enfin, certains commentateurs avancent que le fait d'encadrer le débat sur la réglementation de l'environnement numérique selon l'opposition entre liberté d'expression et censure nuit à la discussion productive sur la manière de traiter les préjudices cyberfacilités très réels et omniprésents examinés dans ce rapport et sur la manière dont les environnements inhibiteurs de parole touchent les groupes racisés et minorisés (Haggart et Tusikov, 2021). La sécurité publique numérique exige que les décideurs politiques s'éloignent de cette vision simplifiée des effets de la réglementation sur le discours (Haggart et Tusikov, 2021). Une approche plus adaptée de la sécurité publique à l'ère numérique consiste à recourir à une combinaison de mesures, notamment la mise en place d'incitations aux entreprises à une meilleure autorégulation et à une protection renforcée des données et de la vie privée (notamment par des lois réglementant une intelligence artificielle (IA) responsable et transparente) (Cusumano *et al.*, 2021) (section 5.2.5).

5.2.1 Australie

La loi sur l'amélioration de la sécurité en ligne de 2015 considère certaines communications numériques comme des infractions criminelles

Le gouvernement australien a introduit la loi sur l'amélioration de la sécurité en ligne (*Enhancing Online Safety Act 2015*) pour répondre aux plaintes relatives aux préjudices en ligne, comme la cyberintimidation des enfants et le partage de « matériel violent odieux » (Commissaire à la sécurité électronique, s.d.a). La loi a créé le commissariat à la sécurité électronique du pays (Gouv. de l'Australie, 2015), dont le rôle consistait à l'origine à protéger les enfants, mais, comme nous le verrons plus loin, a ensuite été élargi pour inclure tout le monde en Australie (Gouv. de l'Australie, 2017). Le commissariat à la sécurité électronique est un bureau indépendant soutenu par l'organe national de réglementation des médias, l'Australian Communications and Media Authority (Gouv. de l'Australie, 2015; Commissaire à la sécurité électronique, s.d.a). Une modification à cette loi — la loi de 2018 sur l'amélioration de la sécurité en ligne (Partage non consensuel d'images intimes) (*Enhancing Online Safety [Non-Consensual Sharing of Intimate Images] Act 2018*) — érige en infraction le partage d'images intimes sans consentement (Gouv. de l'Australie, 2018). Elle interdit également aux personnes de partager, sans consentement, des images où une victime ne porte pas les vêtements qu'elle porte habituellement en public pour des raisons culturelles ou religieuses (p. ex. un sikh sans son turban) (Gouv. de l'Australie, 2018).

Selon la situation, le commissaire à la sécurité électronique dispose de pouvoirs d'enquête et de la capacité de requérir des sanctions civiles ou criminelles, en collaboration avec les forces de l'ordre et les tribunaux (Commissaire à la sécurité électronique, s.d.a). En bref, il constitue un nouveau mécanisme pour traiter certains crimes cyberfacilités en dehors de l'application traditionnelle de la loi. Yar et Drew (2019) notent que « l'approche adoptée en Australie à l'égard des [abus sur Internet], si elle peut souffrir des mêmes lacunes concernant les auteurs que pour d'autres types de cybercrimes, s'est concentrée sur les actes qui relèvent d'une mission réalisable de prévention des nouveaux [abus sur Internet] et sur la perturbation de ce crime » [traduction libre]. Par exemple, le commissaire apporte également son appui aux victimes d'abus par l'image en aidant au retrait d'images ou de vidéos intimes (Commissaire à la sécurité électronique, s.d.a)[13], ce qui, selon Yar et Drew (2019), « peut être le résultat le plus important pour les victimes » [traduction libre]. Le gouvernement canadien a cité le commissaire australien à la sécurité électronique dans ses propositions politiques et législatives, le décrivant comme une source d'inspiration possible pour les réformes nationales (Meyer, 2021).

La loi sur le partage de documents violents et odieux a créé des obligations de signalement aux forces de l'ordre pour les fournisseurs de contenu et d'accès Internet et les hébergeurs

L'Australie a également adopté la loi sur le partage de documents violents et odieux (*Sharing of Abhorrent Violent Material Act*), une modification de la loi de 1995 sur le Code criminel (*Criminal Code Act 1995*), à la suite de l'attentat terroriste de 2019 à Christchurch, en Nouvelle-Zélande (Gouv. de l'Australie, 2019). Cette modification exige que les fournisseurs de contenu et d'accès Internet et les hébergeurs signalent à la police fédérale australienne, « dans un délai raisonnable », les « comportements violents et odieux » qui se produisent en Australie et à partir de leurs serveurs. Elle érige également en infraction le fait pour les fournisseurs de contenu et de services d'hébergement de « ne pas supprimer rapidement l'accès à du contenu violent et odieux » [traduction libre] (Gouv. de l'Australie, 2019).

L'extension des pouvoirs policiers sur Internet permise par la loi sur la sécurité en ligne soulève des inquiétudes en matière de droits de la personne

La loi sur la sécurité en ligne (*Online Safety Act*), entrée en vigueur en janvier 2022, étend les pouvoirs du commissaire à la sécurité électronique en :

13 Le commissaire à la sécurité électronique peut apporter son aide si la personne représentée sur la photo ou la vidéo, ou la personne qui l'a publiée, réside en Australie ou si l'image est hébergée en Australie (Commissaire à la sécurité électronique, s.d.b).

- intégrant l'ensemble des services Internet dans le mécanisme de lutte contre la cyberintimidation (p. ex. par l'inclusion du jeu en ligne et des platesformes de partage de contenu en plus des médias sociaux);
- permettant au commissaire à la sécurité électronique d'exiger le retrait de matériel de cyberabus adulte qui cible un Australien;
- réduisant le délai dont dispose un fournisseur de services pour se conformer à un avis de retrait de 48 heures à 24 heures;
- donnant au commissaire à la sécurité électronique des pouvoirs plus étendus de recueil de renseignements sur l'identité, y compris des renseignements de base sur un abonné pour les comptes anonymes.

Commissaire à la sécurité électronique (2021a)

Bien que le projet de loi ait bénéficié d'un large soutien au sein du parlement australien, le Parti vert s'est opposé aux mesures qu'il contient, déclarant que les pouvoirs étendus du commissaire à la sécurité électronique étaient excessifs. Les Verts ont fait remarquer que « ce projet de loi ferait du commissaire à la sécurité électronique l'unique arbitre du contenu Internet en Australie » [traduction libre] (Mckim, 2021), ajoutant qu'il pourrait en résulter un abus de la procédure de dépôt de plaintes par « des personnes opposées au travail du sexe, à la pornographie et à la santé sexuelle des personnes LGBTIQ+ », de sorte qu'elles « cherchent à faire supprimer le contenu adulte légal en ligne » [traduction libre] (Mckim, 2021).

Une proposition similaire a également soulevé de telles craintes au Canada (Geist, 2021b). Les groupes de défense des droits de la personne ont souligné le potentiel de la loi d'encourager la surveillance automatisée et proactive du contenu par les platesformes de médias sociaux, ce qui peut avoir des conséquences imprévues et dommageables pour les communautés en ligne (DRW, 2021). Cette surveillance pourrait avoir des implications considérables en matière de censure et de liberté d'expression, car il est prouvé que l'automatisation entraîne la suppression d'un volume important de contenu légal (Windwehr et York, 2020). La surveillance proactive peut nuire exagérément aux groupes marginalisés, car les processus automatisés suppriment de manière disproportionnée le contenu produit par certains groupes par rapport à d'autres, à savoir les Noirs, les Autochtones et les personnes LGBTIQ+ (Digital Rights Watch, 2021; Geist, 2021c). Le biais racial dans les modèles d'IA est bien documenté, de multiples études ayant démontré que les Américains noirs sont nettement plus susceptibles de voir leur contenu signalé que les Américains blancs (Davidson *et al.*, 2019; Sap *et al.*, 2019).

Il existe des différences importantes entre les contextes juridiques australien et canadien

Bien que le système juridique australien présente certaines similitudes avec celui du Canada, ses approches peuvent ne pas convenir à la situation canadienne. Une distinction importante entre les systèmes juridiques des deux pays est que l'Australie ne dispose pas d'une déclaration des droits[14]. Les lois canadiennes ne doivent pas enfreindre les dispositions de la *Charte des droits et libertés*, qui fait partie de la *Constitution du Canada* (GC, 2020a). L'absence d'une déclaration des droits a des conséquences pratiques importantes. Par exemple, en 2019, la Haute Cour d'Australie a confirmé le droit du gouvernement australien de mettre fin à l'emploi d'un fonctionnaire en raison de gazouillis négatifs à l'égard de la politique gouvernementale (HCA, 2019; Triggs, 2019). Dans sa décision, le tribunal a noté que, si l'affaire s'était produite au Canada, la *Charte des droits et libertés* aurait pu offrir certaines protections au fonctionnaire (HCA, 2019; Triggs, 2019)[15].

5.2.2 Nouvelle-Zélande

La loi sur les communications numériques préjudiciables considère certaines communications numériques comme des infractions criminelles

En Nouvelle-Zélande, la loi sur les communications numériques préjudiciables (*Harmful Digital Communications Act*, ou HDC Act), adoptée en 2015, traite des préjudices graves en ligne subis à cause des communications numériques (Gouv. de la Nouvelle-Zélande, 2015). En vertu du paragraphe 22(1), une communication est réputée être une infraction criminelle lorsque (i) elle est réputée avoir l'intention de causer un préjudice; (ii) « la publication de la communication causerait un préjudice à une personne raisonnable ordinaire en position de victime » [traduction libre] et (iii) elle a effectivement causé un préjudice (Gouv. de la Nouvelle-Zélande, 2015). Les communications préjudiciables qui n'atteignent pas ce seuil peuvent être traitées dans le cadre d'une poursuite civile (Hunt, 2020). En vertu de la HDC Act, une personne peut signaler un cas de préjudice en ligne qui enfreint les principes légaux relatifs aux communications à Netsafe, un organisme à but non lucratif indépendant qui fournit des conseils et travaille au règlement des plaintes (Netsafe, 2021). En 2020, 556 personnes avaient fait l'objet d'accusations criminelles en vertu de la HDC Act, le nombre d'accusations ayant augmenté au cours des dernières années (on a enregistré 127 accusations en 2020 contre 80 en 2016) (Harris, 2021). La HDC Act a été modifiée à propos du partage

14 Les Australiens possèdent cinq droits individuels inscrits dans la constitution : le droit de vote, la protection contre l'acquisition de biens à des conditions injustes, le droit à un procès devant un jury, la liberté de religion et l'interdiction de la discrimination fondée sur l'État de résidence (Gouv. de l'Australie, 2010; AHRC, s.d.).

15 On ignore si l'issue de l'affaire aurait été la même ou pas au Canada.

d'images intimes non consensuelles par la suppression de la nécessité pour les victimes ou les survivants de démontrer l'existence d'un préjudice (tel que défini dans la Loi). Le partage de telles images sans consentement constitue un crime, sans que les victimes ou les survivants aient à convaincre les tribunaux qu'ils ont subi une « détresse émotionnelle grave » [traduction libre] (Gouv. de la Nouvelle-Zélande, 2015, 2022).

Les modifications apportées à la loi de 1993 sur la classification des films, des vidéos et des publications préviennent et atténuent les préjudices causés par la diffusion en continu en direct de contenu répréhensible

La loi de 1993 sur la classification des films, des vidéos et des publications (*Films, Videos, and Publications Classification Act 1993*) a été modifiée afin de prévenir et d'atténuer les préjudices causés par la diffusion de matériel « répréhensible », tel que du contenu représentant l'horreur, un crime, de la cruauté ou de la violence (Gouv. de la Nouvelle-Zélande, 1993, 2021). Ainsi modifiée, la loi prévoit que la diffusion en continu en direct de contenu répréhensible constitue une infraction criminelle qui s'applique à l'individu ou au groupe qui diffuse le contenu, mais pas aux hôtes du contenu Web tels que les platesformes. Elle donne également aux inspecteurs des publications et au censeur en chef de nouveaux pouvoirs pour limiter la publication et la diffusion de contenu répréhensible (Gouv. de la Nouvelle-Zélande, 2021).

5.2.3 Royaume-Uni

Le projet de loi sur la sécurité en ligne introduit de nouvelles obligations pour les fournisseurs de services Internet

En 2019, le gouvernement du Royaume-Uni a publié un livre blanc sur les méfaits en ligne (*Online Harms White Paper*) (Gouv. du Royaume-Uni, 2019). Bien que, pour rédiger ce document, il ait examiné de près les changements juridiques en Australie, en Allemagne et dans l'Union européenne, l'approche britannique diffère de celle des autres pays en ce qu'elle propose un cadre réglementaire complet pour couvrir une grande variété de crimes et de méfaits cyberfacilités dans un seul document (Gouv. du Royaume-Uni, 2019).

Pour faire face aux crimes et méfaits cyberfacilités mentionnés dans le livre blanc, le secrétaire d'État britannique au Numérique, à la Culture, aux Médias et au Sport a proposé un nouveau cadre réglementaire dans le projet de loi sur la sécurité en ligne (*Online Safety Bill*) (Parlement britannique, 2022a). Ce projet de loi fixe les obligations des fournisseurs de services Internet qui « facilitent le partage de contenu entre utilisateurs ou possèdent un moteur de recherche, ou publient certains éléments de contenu pornographique » [traduction libre] (Judson, 2022).

Bien que les services auraient des obligations différentes selon leur taille et leurs fonctionnalités, tous seraient tenus de s'attaquer aux infractions prioritaires, notamment l'exploitation et les abus sexuels concernant des enfants, le terrorisme, les menaces, le traquage, la publication d'images sexuelles privées et la vente de drogues et d'armes. Ils seraient également tenus d'empêcher les utilisateurs de trouver du contenu illégal prioritaire, de réduire la durée pendant laquelle un tel contenu reste en ligne, d'introduire des mesures d'atténuation et de gestion des risques et de préciser dans leurs conditions d'utilisation « comment les utilisateurs sont protégés du contenu illégal » [traduction libre] (Judson, 2022). En outre, les services auxquels les enfants sont susceptibles d'avoir accès seraient soumis à des obligations supplémentaires, notamment atténuer le risque de préjudice pour les enfants, les empêcher de trouver du contenu préjudiciable et préciser dans les conditions d'utilisation « comment les enfants sont protégés du contenu préjudiciable » [traduction libre] (Judson, 2022).

En vertu de ce projet de loi, les entreprises qui fournissent des services Internet aux utilisateurs du Royaume-Uni seraient tenues de respecter certaines obligations de diligence, notamment en procédant à des évaluations des risques concernant le contenu illégal, en garantissant la liberté d'expression, le respect de la vie privée et la protection du contenu journalistique et en mettant en place des processus de déclaration des plaintes et de tenue de registres (Gouv. du Royaume-Uni, 2021a, 2021c). Il est à noter qu'un projet de loi prévoyait qu'un sous-ensemble comprenant les TIC les plus importantes et les plus populaires serait aussi tenu de traiter spécifiquement le contenu « légal, mais préjudiciable » [traduction libre] (Gouv. du Royaume-Uni, 2021a). Dans la documentation justificative, l'expression « légal, mais préjudiciable » a été définie comme « susceptible d'inclure des problèmes tels que l'abus, le harcèlement ou l'exposition à du contenu favorisant l'automutilation ou les troubles de l'alimentation » [traduction libre] (Gouv. du Royaume-Uni, 2022). Cette disposition a été retirée d'une version ultérieure en raison d'inquiétudes à propos de la liberté d'expression (Sandle, 2022; Parlement du Royaume-Uni, 2022b).

L'actuel organisme de réglementation des médias du Royaume-Uni, l'Office of Communications (Ofcom), serait chargé d'élaborer des codes de pratique détaillés et de veiller au respect de ces exigences (Ofcom, 2020; Gouv. du Royaume-Uni, 2021b). L'Ofcom serait également en mesure d'infliger des amendes aux entreprises en cas de non-respect et pourrait bloquer l'accès à des sites dans certaines conditions. Certains craignent que les nouveaux pouvoirs accordés au secrétaire d'État dans le projet de loi ne menacent l'indépendance de l'Ofcom par rapport à l'ingérence gouvernementale (Perrin *et al.*, 2021).

Le projet de loi sur la sécurité en ligne soulève des craintes en matière de liberté d'expression, de reddition de comptes et de transparence

Comme pour des lois similaires promulguées et proposées dans d'autres pays, les critiques ont soulevé des inquiétudes quant au fait que le projet de loi sur la sécurité en ligne menace la liberté d'expression et donne des pouvoirs de censure discrétionnaires à un organisme administratif (Martin, 2021). Certaines entreprises technologiques ont déclaré qu'elles ne sauraient pas quoi censurer en vertu de ce projet de loi (Fenwick, 2021; Martin, 2021). Selon MacCarthy (2022), il manque également plusieurs éléments importants à ce projet de loi. Une omission notable est l'absence d'accès obligatoire aux données des médias sociaux pour les chercheurs et les auditeurs indépendants. Ce mécanisme indépendant est essentiel pour évaluer la qualité des politiques de modération de contenu des entreprises de médias sociaux. Le projet de loi minimise également le rôle des groupes de la société civile, des universitaires, des experts techniques et des représentants de l'industrie dans la conception réglementaire (MacCarthy, 2022). En décembre 2022, le projet de loi actualisé était en cours d'examen par le Parlement; il pourrait subir d'autres modifications (Parlement du Royaume-Uni, 2022b).

5.2.4 États-Unis

La loi sur la décence des communications donne à chaque fournisseur de services la liberté d'élaborer ses propres politiques de modération du contenu

Les États-Unis étant l'allié international et le partenaire commercial le plus proche du Canada, les décisions de son gouvernement et les mesures qu'il prend peuvent avoir des effets extraterritoriaux sur la population canadienne en encourageant les gouvernements au Canada à adopter des lois similaires, afin de faciliter l'application de la loi et le commerce transfrontaliers. Toutefois, l'approche américaine diffère sensiblement de celle suivie par les autres pays du Groupe des cinq. La politique numérique des États-Unis met l'accent sur la protection de la liberté d'expression en vertu du premier amendement de la Constitution des États-Unis (OCDE, 2020b) et accorde l'immunité aux platesformes de médias sociaux pour certains documents publiés par leurs utilisateurs. Il existe toutefois des limites à cette protection : le Code des États-Unis (United States Code) impose des restrictions au discours qui incite à commettre un crime (18 U.S.C., para 373) (Gouv. des États-Unis, s.d.a), encourage la prostitution ou la traite des êtres humains (18 U.S.C., para 2421A) (Gouv. des États-Unis, s.d.b) ou comprend du matériel d'abus pédosexuels (MAP) (18 U.S.C., para 2251-2260) (Gouv. des États-Unis, s.d.c).

L'article 230 de la loi sur la décence des communications (*Communications Decency Act*), qui est entrée en vigueur en 1996, a été au centre des discussions sur l'atténuation des préjudices en ligne en vertu du droit américain. Il exonère les « fournisseurs de services interactifs » (p. ex. une plateforme de médias sociaux hébergeant du contenu de tiers) de toute responsabilité concernant le contenu publié par les utilisateurs sur leurs platesformes, à une poignée d'exceptions près (Brannon, 2019). Selon Klonick (2018), « l'objectif de l'octroi de cette immunité était à la fois d'encourager les platesformes à être de «bons samaritains» et à jouer un rôle actif dans le retrait du contenu offensant, mais aussi d'éviter les problèmes de liberté d'expression dus à la censure collatérale » [traduction libre]. L'article 230 accorde à chaque fournisseur de services la liberté d'élaborer ses propres politiques de modération du contenu. Ainsi, rien dans cet article n'empêche les fournisseurs de services de retirer et d'interdire certains éléments de contenu (Funk, 2021) et il n'accorde pas non plus d'immunité pour les crimes fédéraux, comme la publication de MAP ou de contenu soutenant le terrorisme. Les platesformes sont soumises à la même responsabilité juridique que tout individu en ce qui concerne la publication de ce contenu. Pour tenir un hébergeur de contenu responsable de la publication de MAP, le gouvernement doit prouver qu'il a sciemment omis de retirer le contenu illégal à l'échelon fédéral. Cependant, la loi n'oblige pas les platesformes à rechercher de manière proactive le matériel illégal (Funk, 2021).

La loi sur la lutte contre le trafic sexuel en ligne (*Fight Online Sex Trafficking Act*), adoptée en 2018, a ajouté à l'article 230 une exception pour le contenu relatif au trafic sexuel et à la prostitution (Chambre des représentants des États-Unis, 2018). Cette disposition peut rendre les platesformes responsables des messages relatifs au travail du sexe. Par conséquent, des sites Web ont commencé à censurer une partie de leurs pages susceptibles d'être utilisées pour des publicités de prostitution (Tripp, 2019). Certains travailleurs du sexe consensuels ont été contraints de se déconnecter, ce qui a pu entraîner une augmentation de la violence à leur égard (Tripp, 2019; Newton, 2020) (encadré 2.3).

L'article 230 continue d'être controversé, et diverses propositions ont été envisagées pour restreindre l'affichage de discours haineux, de contenu terroriste, d'images non consensuelles ou de contenu contribuant au cybertraquage (Newton, 2020). L'Accord Canada-États-Unis-Mexique contient un libellé similaire à celui de l'article 230 (section 5.4).

La loi sur la clarification de l'utilisation licite des données à l'étranger minimise les exigences élémentaires en matière de primauté du droit pour les demandes d'assistance juridique

La loi sur la clarification de l'utilisation licite des données à l'étranger (*Clarifying Lawful Overseas Use of Data Act*, ou CLOUD Act) est une loi fédérale américaine susceptible d'avoir des répercussions mondiales. L'un des objectifs de la Loi est de mieux permettre aux autorités étrangères d'obtenir des données sur les résidents et les citoyens de leur pays détenues par des entreprises américaines. En vertu de cette loi, les États-Unis peuvent conclure des accords bilatéraux avec des pays qui « disposent de solides protections en matière de vie privée et de libertés civiles » [traduction libre] pour obtenir un accès direct aux preuves électroniques (DOJ, 2022a). Le premier accord bilatéral de ce type — signé avec le Royaume-Uni — est entré en vigueur en 2020. En 2019, on avait annoncé que les États-Unis étaient en négociation avec l'Australie et l'Union européenne (DOJ, 2019a,b). En mars 2022, les États-Unis ont entamé des négociations avec le Canada (DOJ, 2022b).

Lorsqu'il existe un accord bilatéral entre les États-Unis et un pays étranger, les forces de l'ordre de l'un ou l'autre des signataires peuvent émettre des mandats ou des assignations pour obliger les entreprises de l'autre pays à fournir des données sur les résidents du pays demandeur (Congrès des États-Unis, 2018). Par exemple, les autorités du Royaume-Uni peuvent avoir accès à des renseignements sur des résidents ou des citoyens britanniques provenant d'entreprises américaines, et inversement. Toutefois, si un organisme d'application de la loi britannique souhaite obtenir des renseignements sur un résident américain auprès d'une entreprise américaine, un traité d'entraide juridique (TAJ) est nécessaire[16]. La CLOUD Act comporte des mécanismes permettant de contester un mandat ou une assignation si l'entreprise estime que la demande enfreint les lois sur la protection de la vie privée du pays où les données sont hébergées (Congrès des États-Unis, 2018).

Certains experts juridiques et défenseurs des droits de la personne affirment que la CLOUD Act n'aborde pas des questions graves concernant l'origine des demandes d'assistance juridique (Guliani et Shah, 2018). Alors que les TAJ imposent aux pays demandeurs des normes en matière de primauté du droit et de droits de la personne, la CLOUD Act minimise ces exigences élémentaires (Evans *et al.*, 2019). La conséquence générale de la CLOUD Act est que les résidents de certains pays demandeurs peuvent être soumis à des normes de protection inférieures à celles dont ils auraient bénéficié en vertu du TAJ. En outre, Guliani et Shah (2018) affirment que certains pays demandeurs pourraient utiliser les renseignements obtenus en vertu de la CLOUD Act pour violer les droits de la personne et cibler les défenseurs de ces droits. Ils ajoutent que l'abandon du

16 Les TAJ sont utilisés par les forces de l'ordre pour mener des enquêtes transfrontalières (Dentons, 2021).

processus d'évaluation des demandes en vertu des TAJ risque d'entraîner une application excessive de la loi et la divulgation de renseignements par l'ensemble des entreprises.

La proposition de loi sur l'élimination de la négligence abusive et généralisée des technologies interactives menace le droit à la vie privée et le droit à la liberté d'expression

La loi sur l'élimination de la négligence abusive et généralisée des technologies interactives (*Eliminating Abusive and Rampant Neglect of Interactive Technologies Act*, ou EARN IT Act) est un texte législatif proposé en 2022 qui cherche à faire en sorte que les fournisseurs de services électroniques obtiennent l'immunité par rapport à l'article 230 mentionné précédemment en ce qui concerne les plaintes relatives au MAP (Congrès des États-Unis, 2022). Dans un tel cas, les fournisseurs doivent démontrer qu'ils respectent l'une des deux « règles refuge » pour pouvoir bénéficier de la protection de cet article. La première règle refuge consiste à mettre en œuvre les pratiques exemplaires fédérales en matière de prévention de l'exploitation des enfants sur Internet. La deuxième consiste à adopter d'autres « mesures raisonnables » en lieu et place des pratiques exemplaires fédérales (Congrès des États-Unis, 2022).

En vertu de la EARN IT Act, le chiffrement de bout en bout pourrait être considéré comme contraire aux pratiques exemplaires ou comme une mesure déraisonnable. En effet, le chiffrement empêche un fournisseur de voir le contenu des fichiers sur son service (Pfefferkorn, 2020; Sly et Wheeler, 2022). Un certain nombre de défenseurs des droits de la personne, d'universitaires et d'organismes s'opposent à la EARN IT Act, arguant que l'interdiction potentielle du chiffrement de bout en bout est contraire au droit à la vie privée. En outre, en menaçant les entreprises technologiques de litige important en cas de conformité insuffisante aux normes de MAP, l'EARN IT Act peut conduire à une censure privée du discours légal, laquelle peut à son tour avoir un effet paralysant sur la liberté de parole et d'expression (Pfefferkorn, 2020). En décembre 2022, cette loi n'avait pas encore été adoptée.

5.2.5 Union européenne

Le Règlement général sur la protection des données (RGPD) a des effets extraterritoriaux

Les instruments réglementaires en matière de données et d'Internet de l'Union européenne (UE) visent avant tout à protéger les intérêts des consommateurs de services numériques. L'UE étant un partenaire stratégique du Canada, ses réformes juridiques peuvent avoir des effets extraterritoriaux quand elles

s'appliquent aux entreprises canadiennes, même celles situées en dehors de l'UE, ou encouragent les décideurs nationaux à introduire des mesures similaires en matière de protection des consommateurs et des données.

Entré en vigueur en mai 2018, le RGPD constitue le texte législatif sur la protection des données le plus complet au monde. Il fait de la protection des données un droit fondamental et promeut le traitement légal des données personnelles et la conformité des entreprises (Jones et Kaminski, 2021). Le RGPD a des effets extraterritoriaux importants (UE, 2016). Premièrement, il s'applique aux responsables du traitement des données étrangers s'ils offrent des biens ou des services à toute personne située ou résidant dans l'UE ou s'ils surveillent le comportement au sein de l'Union. Deuxièmement, il s'applique au traitement des données personnelles par un responsable du traitement des données étranger, lorsque le droit d'un État membre s'applique en vertu d'accords internationaux (p. ex. les affectations consulaires) (UE, 2016). Par conséquent, la portée du RGPD pourrait s'étendre aux entreprises canadiennes situées en dehors de l'UE qui recueillent des données auprès de résidents de l'UE.

Des ambiguïtés importantes subsistent quant à la définition des « données personnelles » selon le RGPD

Le RGPD tente de relever plusieurs défis dans le domaine du droit de la protection des données qui intéressent la réforme du droit canadien. Le premier concerne la signification du terme *données personnelles* face à l'évolution technologique (Laidlaw, 2021b). Le RGPD définit les *données personnelles* de manière large pour inclure les individus directement ou indirectement identifiés et identifiables et établit différentes catégories de données personnelles sensibles (UE, 2016). Cependant, dans certains cas, il n'est pas clair si ce qui est recueilli ou utilisé constitue des données personnelles (Laidlaw, 2021b). Par exemple, si un utilisateur est anonyme, les données recueillies ne sont pas personnelles. Cependant, de nombreux informaticiens affirment que l'anonymisation des données est difficile et qu'un utilisateur peut toujours être identifié à l'aide de techniques d'exploration de données (Ohm, 2010). De plus, les données inférentielles présentent un risque critique pour la vie privée. Les algorithmes d'apprentissage automatique, par exemple, peuvent établir des liens entre des données ordinaires et anonymisées en effectuant sur les individus des inférences qui seraient catégorisées comme personnelles ou sensibles (Wachter et Mittelstadt, 2019). Le RGPD a élargi les catégories de données sensibles pour inclure les données biométriques et génétiques, mais pas les données inférentielles (Laidlaw, 2021b).

On assiste à un mouvement croissant pour améliorer les modèles de consentement dans le RGPD

Le deuxième défi que le RGPD tente de relever et qui intéresse le Canada est l'amélioration des modèles de consentement (Laidlaw, 2021b). Le RGPD prévoit que le consentement doit être « toute manifestation de volonté, libre, spécifique, éclairée et univoque » (UE, 2016), et interdit les modèles à retrait de consentement. En outre, il permet aux personnes concernées de retirer leur consentement, ce qui déclenche un droit à l'effacement (un terme plus précis que le *droit à l'oubli*) (UE, 2016). Malgré les réformes, il y a un mouvement croissant pour remanier les modèles de consentement dans le RGPD et dans d'autres lois sur la protection des données, comme la LPRPDE. Dans l'UE et au Canada, de nombreuses propositions de réforme portent sur la manière d'améliorer le consentement par de meilleures lois, la technologie ou une combinaison des deux. Les propositions de réforme comprennent le renforcement des mécanismes de responsabilisation des entreprises, tels que « la démonstration de la conformité, l'encouragement des codes de pratique industriels, l'utilisation de tiers de confiance pour vérifier les applications et les services et le passage à une approche fondée sur le risque » [traduction libre] (Laidlaw, 2021b). D'autres suggestions incluent la création de « zones interdites », dans lesquelles les organismes ne peuvent pas s'appuyer sur le consentement pour recueillir et traiter des données personnelles (ETHI, 2018). Parmi les idées de garanties technologiques, citons « les codes sur les dispositifs QR qui mènent les consommateurs à des renseignements plus approfondis, les portails ou tableaux de bord gérés par les utilisateurs et l'intégration de la protection de la vie privée dans la conception des produits et services » [traduction libre] (Laidlaw, 2021b).

Le consentement n'est qu'une des conditions légales du traitement des données en vertu du RGPD, et son remaniement ne répond pas à tous les cas dans lesquels les gens peuvent avoir besoin d'une meilleure protection de leurs données. Parmi les autres conditions figurent le traitement nécessaire à l'exécution d'un contrat, le respect d'une obligation légale, la protection des intérêts vitaux de la personne concernée ou d'une autre personne physique, l'exécution d'une mission d'intérêt public ou l'« intérêt légitime » du responsable du traitement (UE, 2016). En pratique, de nombreux responsables du traitement peuvent s'appuyer sur l'intérêt légitime pour leurs activités de traitement des données. La protection contre la fraude, le marketing direct et le traitement des données personnelles dans le but d'améliorer un moteur de recherche peuvent être considérés comme des motifs légitimes de traitement des données, ce qui signifie qu'ils ne nécessitent pas de consentement (Edwards, 2018).

Le RGPD renforce et élargit la portée du droit à l'effacement

Le RGPD vise à donner des pouvoirs aux personnes concernées en codifiant leur droit à l'effacement reconnu par la justice (Laidlaw, 2021b). Ce droit a été confirmé par la Cour de justice de l'Union européenne (CJUE) dans l'affaire *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos, Mario Costeja Gonzalez (Google Spain)*, avant l'entrée en vigueur du RGPD (CJUE, 2014). Dans ce cas, M. Gonzalez a demandé à Google de retirer de ses résultats de recherche un lien vers une ancienne faillite. La CJUE a estimé que Google était un responsable du traitement des données de M. Gonzalez et que ce dernier avait le droit de voir les liens vers ses données supprimées des résultats de recherche lorsque ces données étaient « inadéquates, non ou plus pertinentes ou excessives » [traduction libre] (CJUE, 2014). Le RGPD a non seulement codifié ce droit, mais a également étendu son champ d'application au-delà des moteurs de recherche, confirmant que ce droit peut être invoqué contre tout responsable du traitement des données. En vertu du RGPD, toute personne concernée dispose d'un droit à l'effacement face à tout responsable de traitement, qu'il s'agisse d'une plateforme, d'une grande enseigne ou d'un magasin de proximité. L'affaire a retenu l'attention au Canada, qui s'est demandé si un droit similaire constituait une interprétation légitime de la LPRPDE (Laidlaw, 2021b).

En 2021, Google a adopté une politique mondiale qui permet aux personnes de moins de 18 ans ou à leurs tuteurs de demander le retrait de photos de ses résultats de recherche (Sullivan, 2021). Bien que cette mesure soit similaire au droit à l'effacement du RGPD pour les personnes de moins de 18 ans, la portée du RGPD s'étend aux demandes de suppression de *toutes les données* d'une personne recueillies lorsqu'elle était mineure (CE, s.d.).

La mise en œuvre de la directive sur le commerce électronique varie selon les États membres

La *directive sur le commerce électronique* a été adoptée en 2000 afin d'harmoniser les obligations des services de la société de l'information (UE, 2000)[17]. Ces services bénéficient du même éventail de règles refuges conditionnelles contre la responsabilité qui s'appliquent au « simple transport » et aux fournisseurs se livrant à la « mise en cache » ou à l'« hébergement » de contenu de tiers. C'est pour les hôtes de contenu tiers que les conditions de règle refuge sont les plus complexes. Pour éviter toute responsabilité, ceux-ci ne doivent pas avoir « effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicites est

17 La directive les définit comme tout service fourni, normalement contre rémunération, à distance par moyen électronique, à la demande individuelle d'un destinataire (UE, 2000).

apparente » (UE, 2000). Dans les faits, toutefois, la mise en œuvre de la directive varie fortement d'un État membre à l'autre, les lois nationales en matière de responsabilité restent très fragmentées et les États membres ne savent pas très bien comment l'appliquer compte tenu de la prolifération de nouveaux types de services en ligne, tels que les entreprises de médias sociaux (Madiega, 2020, 2021).

La législation sur les services numériques modernise le régime des services en ligne

En 2022, l'UE a adopté la *législation sur les services numériques*, qui vise à harmoniser les obligations des services en ligne, à fixer des normes plus élevées en matière de responsabilité et de transparence, à imposer des obligations de gestion des risques et à lutter contre les méfaits en ligne (UE, 2020; Madiega, 2021; CE, 2022a). Cette législation concerne principalement les intermédiaires et les platesformes, tels que « les places de marché en ligne, les réseaux sociaux, les platesformes de partage de contenus, les boutiques d'applications et les platesformes de voyage et d'hébergement en ligne » (Allen et Overy, 2020; CE, 2022a).

Ses dispositions les plus importantes sont celles qui obligent les platesformes à atténuer le risque de préjudice, notamment en imposant des rapports sur la transparence et des obligations spéciales pour les très grandes platesformes (UE, 2020; CE, 2022b). Les rapports sur la transparence en matière de modération du contenu doivent contenir des renseignements sur les ordonnances gouvernementales, les signalements par les utilisateurs, les mesures prises par les services de leur propre initiative et les mesures contre l'utilisation abusive des outils de modération automatisée du contenu (Nosák, 2021). Ils permettront aux chercheurs, aux organismes de surveillance et au public de mieux comprendre le processus de modération du contenu, notamment de savoir qui effectue des signalements et pourquoi et les motifs de retrait de certains éléments de contenu (Nosák, 2021). En outre, les très grandes platesformes en ligne (celles qui comptent plus de 45 millions d'utilisateurs actifs mensuels dans l'UE) sont soumises à des obligations spéciales concernant la diffusion de contenu illégal et préjudiciable. Elles sont tenues de mettre en place des mécanismes de modération du contenu, de faire connaître leurs algorithmes de classement du contenu et de donner aux utilisateurs la possibilité de modifier les paramètres de classement du contenu (Allen et Overy, 2020; PE, 2022). La *législation sur les services numériques* modernise également le régime de responsabilité des intermédiaires en ligne en exigeant que chaque fournisseur d'hébergement ou plateforme Web crée des mécanismes de notification et de retrait de contenu illicite (UE, 2020). Si un tel contenu est retiré, l'intermédiaire sera tenu de fournir une explication à la personne qui a téléversé le contenu.

Les exigences d'interopérabilité de la législation sur les marchés numériques peuvent affaiblir ou compromettre la sécurité et le chiffrement de bout en bout

La *législation sur les marchés numériques* est une loi visant à limiter le pouvoir des grandes entreprises technologiques qui ont une capitalisation boursière de plus de 75 milliards d'euros et plus de 45 millions d'utilisateurs dans l'UE (Faife, 2022). Entre autres choses, elle contient une exigence d'interopérabilité pour les applications de messagerie. Plus précisément, plusieurs « contrôleurs d'accès » — Apple, Google, Meta et Microsoft — seront tenus d'assurer l'interopérabilité de leurs services de messagerie avec d'autres applications lorsque leurs concurrents en feront la demande. L'objectif de l'interopérabilité est de permettre aux utilisateurs de passer plus facilement de la plateforme d'un contrôleur d'accès à une plateforme concurrente, sans pour autant entraver leur capacité à se connecter avec les utilisateurs qui souhaitent rester sur les grandes platesformes. En tant que telle, l'interopérabilité diminue le pouvoir que les contrôleurs d'accès exercent sur leurs utilisateurs et donne aux nouveaux services une chance de rivaliser (Stoltz *et al.*, 2022).

L'accès à plusieurs applications et services de messagerie peut protéger les utilisateurs contre la surveillance et la censure gouvernementales et améliorer la qualité des services (Stoltz *et al.*, 2022). En effet, les nouvelles applications peuvent offrir des fonctionnalités de pointe qui renforcent la vie privée des utilisateurs et proposent des conditions d'utilisation conviviales. Toutefois, l'exigence d'interopérabilité pour la messagerie chiffrée peut affaiblir ou compromettre la sécurité et le chiffrement de bout en bout, ce qui pourrait avoir une incidence négative sur tous les utilisateurs (section 6.3). La *législation sur les marchés numériques* démontre qu'une solution technologique relativement simple à exprimer sous forme de politique peut avoir des conséquences imprévues sur la sécurité et les droits de la personne (Stoltz *et al.*, 2022). En ce sens, elle pose des défis similaires aux propositions américaines, qui facilitent l'accès des forces de l'ordre aux données chiffrées (section 5.2.4).

5.2.6 Allemagne

La loi visant à améliorer l'application de la loi sur les réseaux sociaux limite la diffusion en ligne de contenu illégal

La loi visant à améliorer l'application de la loi sur les réseaux sociaux (*Netzwerkdurchsetzungsgesetz*, ou NetzDG) est l'un des textes législatifs sur les méfaits en ligne les plus analysés et les plus influents. Elle a été adoptée en 2017 pour limiter la diffusion en ligne de contenu illégal déjà défini, tel que les représentations de la violence, le MAP et les « symboles d'organisations anticonstitutionnelles et terroristes » [traduction libre], notamment les symboles

et la propagande nazis (Gouv. de l'Allemagne, 1998; Parlement allemand, 2017). Elle a été promulguée à la suite des multiples efforts d'introduction d'un système d'autorégulation déployés par les entreprises de médias sociaux afin de réduire le discours haineux sur leurs platesformes (Heldt, 2019). Au moment de son entrée en vigueur, la loi était considérée comme « sans doute la tentative la plus ambitieuse d'un État occidental pour tenir les platesformes de médias sociaux responsables de la lutte contre le discours en ligne jugé illégal en vertu du droit national » [traduction libre] (Tworek et Leerssen, 2019).

La NetzDG exige que les fournisseurs de réseaux sociaux ayant 2 millions d'utilisateurs enregistrés ou plus en Allemagne suivent un ensemble de règlements, dont le non-respect peut valoir des sanctions monétaires importantes (Parlement allemand, 2017). En vertu de la loi, les platesformes doivent disposer d'un mécanisme de signalement permettant aux utilisateurs de déposer des plaintes relatives au contenu; une fois une plainte reçue, la plateforme doit examiner le contenu et le supprimer s'il est jugé illégal. La NetzDG n'a pas créé de nouvelles infractions criminelles concernant la haine en ligne, mais plutôt de nouvelles règles d'application pour les grandes entreprises. Le matériel manifestement illicite doit être retiré dans les 24 heures, tandis que tous les autres éléments de contenu illégaux doivent être retirés dans les 7 jours (Parlement allemand, 2017). À titre de comparaison, le projet fédéral canadien initial de lutte contre le contenu préjudiciable en ligne proposait un délai de 24 heures pour le retrait des cinq catégories suivantes de contenus préjudiciables : « le contenu terroriste, le contenu incitant à la violence, le discours haineux, le partage non consensuel d'images intimes et le contenu d'exploitation sexuelle des enfants » (GC, 2022d). La proposition a été critiquée comme étant trop rigoureuse et encourageant une surcensure du contenu non préjudiciable (Andrey *et al.*, 2021b; Geist, 2021a; GC, 2022d).

La NetzDG a conduit les platesformes à bloquer du contenu légal sur leurs sites en Allemagne

Comme les autres lois qui régissent le contenu préjudiciable, la NetzDG a suscité la controverse. Les critiques ont fait valoir qu'elle pourrait porter atteinte à la liberté de la presse et à la liberté d'expression et avoir des effets négatifs imprévus (p. ex. servir d'exemple aux régimes autoritaires pour restreindre davantage le discours). La disposition sur le retrait dans les 24 heures a suscité des inquiétudes quant au risque de surblocage et de censure de contenu non préjudiciable, ainsi que des questions sur la « privatisation du système judiciaire en raison de l'interprétation et de l'application du droit criminel par des entreprises privées » [traduction libre] (Heldt, 2019). Heldt (2019) note que ces deux résultats pourraient avoir un effet paralysant sur le discours.

Une analyse réalisée par Tworek et Leerssen (2019) a révélé que « les critiques de l'industrie technologique, des activistes et des universitaires semblaient l'emporter sur le soutien » [traduction libre]. Par exemple, comme pour les autres lois ou propositions prévoyant un délai de réaction des platesformes face au contenu signalé, l'exigence de retrait allemande a été critiquée pour avoir incité les platesformes à retirer un trop fort volume de contenu (HRW, 2018). Reporters sans frontières (2018) signale que cette loi a conduit Meta, Twitter et Google à bloquer du contenu légal sur ses sites en Allemagne. La majorité des retraits découlant de plaintes étaient toutefois dus à des violations des directives internes ou des conditions de service des platesformes plutôt qu'à des infractions au droit allemand (Tworek et Leerssen, 2019). Le contenu signalé est d'abord évalué en fonction des directives communautaires, avant que sa légalité en Allemagne ne soit examinée. Comme l'expliquent Tworek et Leerssen (2019), « dans cette optique, il se peut que l'effet le plus important de la NetzDG ait été d'assurer une suppression plus rapide et plus cohérente du contenu en Allemagne en vertu des directives communautaires des entreprises » [traduction libre].

Une modification controversée de la NetzDG oblige les platesformes à signaler le discours haineux aux forces de l'ordre

En juin 2021, la loi modifiant la loi visant à améliorer l'application de la loi sur les réseaux sociaux (*Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes*) est entrée en vigueur. Cette modification place les platesformes de partage de vidéos sous la juridiction de la NetzDG, accroît les exigences en matière de renseignements pour les fournisseurs de médias sociaux, exige que ces entreprises améliorent la convivialité de leurs canaux de signalement de contenu illicite et introduit une procédure de recours en cas de suppression ou de blocage de l'accès au contenu par les entreprises (Library of Congress, 2021). Cette réforme intègre les dispositions de la *directive « Services de médias audiovisuels »* de l'UE dans le droit allemand (Etteldorf, 2021).

Plusieurs entreprises de médias sociaux ont poursuivi le gouvernement allemand pour les modifications apportées au NetzDG, qui obligent les platesformes à signaler de manière proactive le discours haineux aux forces de l'ordre. Un tribunal allemand s'est prononcé en faveur des entreprises au motif que les modifications étaient contraires à la législation de l'UE (Reuters, 2022). Toutefois, cette décision ne s'applique qu'aux parties à la procédure et ne change pas la loi. Les parties peuvent faire appel de cette décision devant les tribunaux supérieurs (Justiz Online, 2022).

5.3 Coopération internationale

Les mécanismes de coopération bilatérale et multilatérale sont axés sur la collaboration entre les services de renseignement nationaux et les forces de l'ordre. Par exemple, certains pays, dont le Canada, se sont efforcés de renforcer la coopération internationale et d'harmoniser leur droit criminel autour de la Convention de Budapest (encadré 5.4).

Encadré 5.4 La Convention de Budapest sur la cybercriminalité

La Convention sur la cybercriminalité, ouverte à la signature depuis 2001, est le premier traité international destiné à lutter contre la cybercriminalité en harmonisant les lois, en soutenant l'application des lois et les poursuites au niveau national et en renforçant la coopération entre les signataires (CdE, s.d.a,b). En janvier 2022, 66 États étaient parties à la Convention, dont la plupart des pays de l'UE, l'Australie, le Canada, le Royaume-Uni et les États-Unis. Le Canada est l'un des premiers signataires, il a ratifié la Convention en 2015 (CdE, 2022).

La Convention a deux objectifs principaux : fournir des lignes directrices aux pays qui élaborent une législation sur la cybercriminalité et servir de cadre juridique à la coopération entre les parties (CdE, 2021a). En outre, selon le Conseil de l'Europe, « [i]l semble que les entités du secteur privé sont également plus susceptibles de coopérer avec les autorités de justice pénale des Parties à la Convention dans la mesure où celles-ci doivent mettre en place un cadre juridique interne sur la cybercriminalité et les preuves électroniques » (CdE, 2021a).

En 2006, un protocole additionnel est entré en vigueur, qui étend le champ d'application de la Convention aux infractions liées à la propagande raciste ou xénophobe (CdE, 2021b). Un autre protocole encore vise à favoriser une plus grande coopération de la part des fournisseurs de services Internet et la divulgation des preuves électroniques (CdE, 2021c). Le protocole prévoit « une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaine et pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés, des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic, la coopération immédiate en cas d'urgence, des outils d'entraide, mais aussi des garanties en matière de protection des données à caractère personnel » (CdE, 2021c). Les groupes de la société civile ont toutefois critiqué ces dispositions, ainsi que les procédures d'adoption (Gullo et Rodriguez, 2021). Le protocole additionnel a été ouvert à la signature en mai 2022.

Des efforts de coopération internationale sont déployés dans le cadre du G7 et du Groupe des cinq

Au-delà de la Convention de Budapest, le Canada est engagé dans des efforts de coopération internationale dans le cadre du G7 et du Groupe des cinq (Dizboni et Leuprecht, 2020). Les membres du G7 se sont engagés à mettre en œuvre les résolutions du Conseil de sécurité des Nations Unies qui portent, entre autres, sur la prévention de l'extrémisme violent et de l'utilisation d'Internet à des fins terroristes. Notamment, leurs ministres de la sécurité se sont concentrés sur la prévention de la propagation d'idéologies haineuses en ligne et ont souligné l'importance de la collaboration avec le secteur privé (p. ex. Meta, Twitter, Google et Microsoft) (Dizboni et Leuprecht, 2020). Dans une déclaration publiée en 2018, les ministres de la Sécurité ont énuméré un certain nombre de mesures, notamment « la suppression du contenu et des comptes dans l'heure suivant leur téléchargement, lorsque cela est techniquement possible, sans compromettre l'exactitude » et la prévention de « la réapparition de contenus extrémistes violents et terroristes en contribuant à la base de données condensées numériques de l'industrie, en l'utilisant et en publiant des mesures de performance » (GC, 2018b). Comme pour les exigences de retrait nationales, les propositions du G7 sur le retrait accéléré du contenu font craindre une censure privée du discours légal et peuvent avoir un effet paralysant sur la liberté d'expression.

Dans un communiqué commun publié en 2017, les ministres et procureurs généraux du Groupe des cinq ont souligné la nécessité d'une stratégie commune de travail avec les fournisseurs de services de communication afin de limiter la propagation des activités et de la propagande terroristes en ligne (SP, 2017a). Ils ont également soutenu la création d'un forum industriel dirigé par Google, Meta, Microsoft et Twitter. Pour faire face aux difficultés que le chiffrement pose à la sécurité publique, le Groupe des cinq a exhorté les entreprises technologiques à concevoir des portes dérobées pour permettre aux forces de l'ordre d'accéder aux messages chiffrés, mais il s'est heurté à des inquiétudes concernant les droits de la personne et le droit à la vie privée (SP, 2017a) (section 6.3). Certains ont noté que le Groupe des cinq constitue un meilleur forum pour l'établissement d'objectifs de coopération plus concrets et plus ambitieux que le G7, car ce dernier est plus diversifié géographiquement et vise à influencer une variété d'États en intégrant les documents des Nations Unies dans son processus de définition des objectifs (Dizboni et Leuprecht, 2020).

L'Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne est un exemple de coopération internationale

La Nouvelle-Zélande a pris la tête des efforts internationaux avec le lancement de l'Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne. Cette initiative est une cocréation des gouvernements néo-zélandais et français en réaction à l'attentat terroriste de 2019 contre la communauté musulmane de Christchurch, en Nouvelle-Zélande (Appel de Christchurch, 2021). Elle encourage les gouvernements et organisations à limiter volontairement la diffusion de contenu terroriste et extrémiste violent « dans le respect de l'état de droit et du droit international des droits de l'Homme » (Appel de Christchurch, 2021). En 2021, 48 pays (dont le Canada), 10 entreprises technologiques, la Commission européenne et 2 organisations internationales se sont joints à l'Appel (Appel de Christchurch, 2021), qui demande aux pays participants d'élaborer et de soutenir des politiques qui contrent les facteurs qui motivent l'extrémisme et le terrorisme, d'appuyer des cadres qui minimisent l'amplification du contenu terroriste et extrémiste violent et d'appliquer les lois qui interdisent ce contenu (Appel de Christchurch, 2019).

5.4 Politique et législation proposées pour lutter contre les méfaits en ligne au Canada

Au Canada, diverses propositions de politique sur la façon d'aborder les méfaits en ligne ont refait surface et évolué au fil des ans, mais l'activité législative sur cette question s'est accélérée en 2020. De nombreuses propositions émanant de décideurs, en réponse aux crimes et méfaits cyberfacilités, préconisent des réformes de portée différente — d'une refonte complète du cadre réglementaire (p. ex. la réglementation des fournisseurs de services de communication en ligne) à des mesures distinctes visant à réglementer différentes activités préjudiciables (p. ex. le traitement du discours haineux comme pratique discriminatoire en vertu de la *Loi canadienne sur les droits de la personne*). La plupart de ces propositions se concentrent sur la conception du mécanisme réglementaire de surveillance des espaces numériques et sur l'attribution de fonctions à des organismes gouvernementaux existants ou nouveaux, tels que le CRTC, la Commission canadienne des droits de la personne et la Commission à la sécurité numérique du Canada.

Une charte numérique non juridiquement contraignante contient des principes relatifs à la sécurité publique numérique

En 2019, le ministère de l'Innovation, des Sciences et du Développement économique (ISDE) a rendu publique la *Charte numérique du Canada en action : un plan par des Canadiens, pour les Canadiens* (ISDE, 2019). La Charte numérique est une déclaration de politique non exécutoire, qui comprend dix principes (figure 5.1) destinés à « orienter le travail du gouvernement fédéral, en servant de charte du numérique pour les Canadiens qui aidera à relever les défis tout en exploitant les talents et les points forts uniques du Canada afin d'utiliser le pouvoir de la transformation du numérique et des données » (Choi, 2019; ISDE, 2019). Elle reconnaît que plusieurs éléments sont essentiels à la sécurité publique, notamment la sûreté et la sécurité, la protection contre la haine et l'extrémisme violent, une application rigoureuse et une réelle responsabilisation (ISDE, 2019). La Charte numérique admet également l'importance de protéger les droits individuels, y compris le droit à la vie privée. Elle vise à éclairer une législation spécifique et, à ce titre, ne contient aucun mécanisme de protection de la vie privée juridiquement applicable et ne donne pas aux gens plus de maîtrise sur leurs données (Choi, 2019; Dubois et Martin-Bariteau, 2020b).

Reproduit avec l'autorisation d'IDSE (2019)

Figure 5.1 Les dix principes de la Charte numérique du Canada

Les dix principes de la Charte numérique du Canada sont le fruit d'une consultation nationale de quatre mois.

5.4.1 Propositions législatives sur le contenu numérique, les méfaits en ligne et la vie privée

Plusieurs projets de loi portant sur le contenu numérique, les méfaits en ligne et la vie privée ont été introduits ou proposés au Canada depuis la publication de la Charte numérique. Par exemple, au cours de la 43e législature (décembre 2019–août 2021) (Chambre des communes du Canada, s.d.), les projets de loi C-10 (2020), C-11 (2020) et C-36 (2021) ont proposé des modifications à la législation sur le contenu en ligne, la protection de la vie privée et le discours haineux, respectivement, tandis que la proposition fédérale visant à lutter contre le contenu préjudiciable en ligne (section 5.2.6) a suggéré de nouveaux mécanismes pour faire face aux méfaits sur Internet. Tous ces projets de loi sont morts au feuilleton (c.-à-d. qu'ils n'ont pas été adoptés pendant la session) après le déclenchement de l'élection fédérale à l'automne 2021, bien que certains aient été réintroduits dans des formats essentiellement semblables lors de sessions parlementaires ultérieures. Le comité d'experts ne les aborde que brièvement, sous l'angle des difficultés qu'ils cherchent à surmonter et de l'approche générale qu'ils suivent.

Les propositions visant à réglementer le contenu audio et audiovisuel en ligne avaient une portée excessive et portaient atteinte à la liberté d'expression

En 2020, le gouvernement a présenté le projet de loi C-10 *(Loi modifiant la Loi sur la radiodiffusion et d'autres lois en conséquence)*, dont l'objectif était que les fournisseurs de contenu audio et audiovisuel en ligne relèvent de la *Loi sur la radiodiffusion* (Brideau *et al.*, 2020; Chambre des communes du Canada, 2021). Cette dernière définit les rôles et les pouvoirs du CRTC en ce qui concerne la réglementation et la supervision de la radiodiffusion au Canada. Actuellement, elle s'applique aux radiodiffuseurs traditionnels « en direct ». Cela signifie que les services Web, tels que Netflix et Spotify, ne sont pas soumis aux mêmes exigences que les stations de télévision et de radio traditionnelles. Le projet de loi C-10 (2020) aurait étendu les règles destinées à promouvoir le contenu canadien dans les environnements de radiodiffusion terrestre aux services Internet (appelés « entreprises en ligne »). Il a fait l'objet d'importantes critiques au motif qu'il permettrait indûment au gouvernement de réglementer la liberté d'expression des individus ou d'interférer avec elle ainsi que d'entraver la capacité des créateurs canadiens à réussir sur les platesformes en ligne, et est finalement mort au feuilleton (Raman-Wilms et Curry, 2021; Smith, 2021b; Geist, 2022a).

En février 2022, le projet de loi a été réintroduit durant la 44e législature, sous le nom de *Loi sur la diffusion continue en ligne* (C-11). Le gouvernement fédéral a fait valoir que le nouveau projet de loi abordait les questions controversées de la version précédente concernant le contenu produit par les utilisateurs. Le ministre

du Patrimoine canadien, Pablo Rodriguez, a déclaré que le projet de loi ne toucherait pas les utilisateurs, les créateurs en ligne ou les créateurs de contenu numérique, mais seulement les platesformes qui hébergent le contenu (Carbert, 2022; Gilmore, 2022). La proposition a reçu un accueil mitigé. L'Association canadienne de la musique indépendante et d'autres groupes de l'industrie de la musique semblaient généralement soutenir le projet de loi pour sa capacité à protéger et à permettre le développement des musiciens et des artistes canadiens (Gilmore, 2022). Elle a toutefois affirmé que C-11 (2022) ne corrigeait pas les problèmes fondamentaux de C-10 (2020) (Bhullar, 2022). Une des préoccupations soulevées par les experts juridiques est l'incertitude créée par la formulation du projet de loi; par exemple, il pourrait concerner tout service audiovisuel mondial ayant des clients canadiens (Geist, 2022a). En outre, bien que le projet de loi prévoie des exemptions pour le contenu produit par les utilisateurs, il inclut également des critères de non-exemption de ce contenu et des indications minimales sur la manière dont ces critères seraient appliqués (Geist, 2022a).

Le projet de loi C-11 (2020) *(Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois)* est un autre texte législatif canadien non adopté. Il avait notamment pour objectif de moderniser la façon dont les données personnelles et la vie privée sont traitées dans le secteur privé au Canada, face à la prolifération des données et des applications numériques (GC, 2020c). Dans les commentaires sur le projet de loi C-11 (2020), y compris de la part d'universitaires et du CPVP, on soutient que, bien qu'il représente une modification nécessaire de la législation canadienne sur la protection de la vie privée, il ne traite pas adéquatement du consentement valable, de la dépersonnalisation des données ou de la mobilité (portabilité) des données (p. ex. Kenyon, 2021; CPVP, 2021b; Scassa, 2021). Le CPVP a fait remarquer que la tentative du projet de loi d'aborder les questions de protection de la vie privée associées à l'économie numérique était mal adaptée et procurait une protection moindre que les approches adoptées dans d'autres pays (CPVP, 2021b).

L'objectif du projet de loi C-36 était de protéger les Canadiens contre le discours haineux dans un environnement numérique

En 2021, le projet de loi C-36 proposait de lutter contre la haine en ligne en modifiant le *Code criminel* et la *Loi canadienne sur les droits de la personne.* Le changement à la *Loi canadienne sur les droits de la personne* était fait :

> *pour énoncer que le fait de communiquer ou de faire communiquer un discours haineux au moyen d'Internet ou de tout autre mode de télécommunication dans un contexte où ce discours haineux est susceptible de fomenter la détestation ou la diffamation d'un individu ou d'un groupe d'individus sur le fondement d'un motif de distinction illicite constitue un acte discriminatoire.*
>
> GC (2021h)

Cette modification aurait permis à la Commission canadienne des droits de la personne d'admettre les plaintes relatives à la haine en ligne diffusée par des fournisseurs de services de communication sur Internet, en lui donnant le pouvoir « de trancher les plaintes et d'ordonner des mesures de réparation » en lien avec des infractions commises sur le Web (GC, 2021). Le projet de loi C-36 (2021) est lui aussi mort au feuilleton, lors de la dissolution du Parlement en août 2021 (Smith, 2021b).

La proposition visant à contrer le contenu en ligne préjudiciable empiète sur les droits constitutionnels

Le plan le plus complet pour contrer les méfaits en ligne au Canada est la proposition fédérale de lutte contre le contenu préjudiciable sur Internet, qui (comme indiqué à la section 5.2.6) visait à procurer de nouveaux mécanismes pour cinq catégories de contenu : « contenu terroriste, contenu incitant à la violence, discours haineux, partage non consensuel d'images intimes, contenu d'exploitation sexuelle des enfants en ligne » (GC, 2021g). La nature de la proposition donne à penser que le gouvernement du Canada s'est inspiré de la législation d'autres pays, notamment de l'Allemagne et de l'Australie (Meyer, 2021; Tworek, 2021b) (section 5.2). Les principales entités à réglementer dans le cadre de cette proposition sont les fournisseurs de services de communication en ligne (FSCL). Ces services sont définis comme des services « accessibles à partir du Canada, qui ont pour objet principal de permettre à un utilisateur de ces services de communiquer par Internet » (GC, 2021i). Cette définition vise spécifiquement à inclure les grandes platesformes, telles que Facebook, YouTube, Pornhub et Twitter, et à exclure les outils en ligne qui ne sont pas des fournisseurs de communication (p. ex. les applications de mise en forme, les sites Web de commentaires sur les voyages), les communications privées et les fournisseurs de services de télécommunications (GC, 2021g). Pour le comité d'experts, on ne sait

pas très bien comment le gouvernement en est arrivé à ses conclusions, car un grand nombre de sites Internet exclus présentent des fonctionnalités ressemblant à celles des sites Web et des services à prendre en considération dans le cadre du plan.

Les FSCL seraient tenus de « prendre toutes les mesures raisonnables » pour s'assurer que le contenu préjudiciable est inaccessible aux utilisateurs au Canada, y compris « tout ce qui est raisonnable et en leur pouvoir » pour l'autosurveillance de leur plateforme en ce qui a trait au contenu préjudiciable. Les FSCL devraient examiner le contenu signalé par les utilisateurs dans les 24 heures et le retirer si ce contenu répond à la définition d'un contenu devant « être rendu inaccessible » du règlement. Les FSCL seraient également tenus de mettre en place des systèmes de recours pour les auteurs de contenu et les personnes ayant signalé du contenu (GC, 2021g).

La proposition prévoit la création d'une Commission à la sécurité numérique du Canada, qui appuierait trois nouvelles entités chargées de surveiller et de faire appliquer les nouvelles règles : un commissaire à la sécurité numérique, un Conseil de recours en matière numérique du Canada et un Comité consultatif. Le commissaire serait chargé d'administrer et de faire respecter les nouvelles exigences, d'étudier les plaintes des utilisateurs de FSCL au sujet du contenu en ligne, de produire des ordres de conformité, de contrôler la conformité des FSCL aux règlements et aux décisions et d'infliger des amendes en cas de non-conformité (GC, 2021i). Dans les cas extrêmes de non-conformité liés à l'exploitation sexuelle des enfants ou au contenu terroriste, le commissaire pourrait demander à la Cour fédérale de bloquer une partie ou la totalité d'un FSCL au Canada. Le Conseil de recours en matière numérique du Canada proposé constituerait un mécanisme indépendant permettant aux utilisateurs de FSCL de faire appel des décisions de modération du contenu prises par un FSCL (GC, 2021g). Le commissaire à la sécurité numérique et le Conseil de recours en matière numérique seraient tous deux soutenus par le Comité consultatif (GC, 2021g).

Outre les règlements et les organismes de réglementation susmentionnés, la proposition comprend des modifications de la loi actuelle concernant les méfaits en ligne. Elle introduit des modifications à la *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*, qui obligent les fournisseurs de services Internet à signaler aux autorités les cas de MAP hébergés sur leurs serveurs (GC, 2011a) et les liens vers les MPA non hébergés sur leur service au Centre canadien de protection de l'enfance (CCPE) (GC, 2011b). Les modifications apportées à la loi comprennent, entre autres, la centralisation du signalement du MAP par le Centre national contre l'exploitation des enfants (CNCEE) de la GRC, comme l'a recommandé le Comité permanent de l'accès à l'information, de la protection des renseignements

personnels et de l'éthique de la Chambre des communes (ETHI, 2021), la clarification du fait que la loi s'applique à tous les types de services Internet (y compris aux FSCL), l'allongement de l'exigence de conservation des données informatiques de 21 jours à 12 mois et l'ajout d'une exigence selon laquelle les « personnes qui fournissent un service Internet » devaient fournir des renseignements supplémentaires au CNCEE (l'autorisation judiciaire n'étant pas une exigence) dans les cas où une infraction de pornographie juvénile était détectée (GC, 2021g; Parsons, 2022). Il n'est pas clair si ces renseignements supplémentaires doivent inclure les renseignements de base sur l'abonné ou les données de transmission (GC, 2021c). Toutefois, certains experts ont affirmé que « les obligations de signalement et de conservation sont d'une utilité limitée », car les forces de l'ordre n'ont ni le temps ni les ressources nécessaires pour traiter tous les contenus signalés et « les recouper avec des informations hors ligne » (GC, 2022e).

Enfin, la proposition fédérale comprend des modifications à la *Loi sur le Service canadien du renseignement de sécurité*, qui prévoient un nouveau mécanisme permettant au SCRS de recevoir plus rapidement l'autorisation d'obtenir des renseignements de base sur les abonnés (GC, 2021i). L'autorisation serait délivrée par un juge de la Cour fédérale et soumise à une surveillance ministérielle (GC, 2021g).

En février 2022, le gouvernement fédéral a publié un rapport résumant les commentaires reçus sur la proposition et a reconnu l'existence d'un certain nombre de « préoccupations générales [...] liées à la liberté d'expression, au droit à la vie privée, à l'impact de la proposition sur certains groupes marginalisés et, plus généralement, [au] respect de la *Charte canadienne des droits et libertés* » (GC, 2022d). En mars 2022, le gouvernement du Canada a nommé un groupe consultatif d'experts ayant pour mandat, entre autres, de suggérer des changements à cette proposition (GC, 2022f).

Le projet de loi C-27 (2022) ne répond pas entièrement aux préoccupations des défenseurs de la vie privée

En 2022, le gouvernement du Canada a présenté le projet de loi C-27 *(Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*) (Chambre des communes du Canada, 2022). Il s'agit d'une version révisée de l'ancien projet de loi C-11 (2020) mort au feuilleton avant l'élection fédérale de 2021 (Alavi *et al.*, 2022). Le projet de loi C-27 (2022) est une proposition de réforme complexe portant, entre autres, sur la dépersonnalisation des données, la réforme du consentement comme fondement de l'utilisation des données et la facilitation de l'usage des données par les secteurs privé et public (Geist, 2022b).

La proposition de *Loi sur la protection de la vie privée des consommateurs* (qui remplacerait la LPRPDE) ne s'applique pas aux données anonymisées et fournit peu de renseignements sur la façon dont les organisations devraient procéder à l'anonymisation (Scassa, 2022a). Elle tente également d'intégrer dans la loi canadienne sur la protection de la vie privée un fondement d'« intérêt légitime » pour le traitement des données, que prévoit le RGPD. Cependant, par rapport à ce dernier, le projet de loi C-27 (2022) fait de l'exception de l'« intérêt légitime » un fondement potentiellement plus courant pour l'utilisation de données personnelles « à l'insu de l'intéressé ou sans son consentement » [traduction libre] (Scassa, 2022b). En outre, les dispositions visant à faciliter l'utilisation par le gouvernement des données du secteur privé ne contiennent pas de protections adéquates de la vie privée collective ou individuelle et minimisent la protection offerte par les lois en vigueur (Scassa, 2022c).

Les obligations du Canada concernant la responsabilité des intermédiaires en vertu de l'Accord Canada-États-Unis-Mexique (ACEUM) ne sont pas claires

La responsabilité des intermédiaires est une question complexe, qui recoupe différentes juridictions et différents domaines du droit. Le Canada ne dispose pas de loi générale sur la responsabilité des intermédiaires comme celles de l'Union européenne ou la *directive sur le commerce électronique* et l'article 230 de la loi sur la décence des communications aux États-Unis; la responsabilité des intermédiaires s'y est plutôt développée dans les dispositions de la common law sur la diffamation et sur le droit d'auteur (Laidlaw, 2021b). En outre, l'article 19.17 de l'ACEUM exige que les parties fournissent aux intermédiaires en ligne une protection contre la responsabilité liée au fait qu'ils hébergent du contenu généré par les utilisateurs (GC, 2020d). Le libellé de cette disposition s'inspire de l'article 230 de la loi sur la décence des communications. Cependant, l'ACEUM n'intègre pas l'article 230 dans le droit canadien. Il permet une interprétation nationale de ces dispositions, et une partie peut respecter l'article 19.17 par le biais de ses lois et de ses règlements ou de l'application judiciaire des doctrines juridiques existantes (Ha-Redeye, 2021). Certains experts juridiques recommandent d'introduire au Canada une législation qui clarifierait la façon dont l'article 19.17 de l'ACEUM est appliqué en général, et aux intermédiaires canadiens et de pays tiers en particulier (Krishnamurthy *et al.*, 2020).

5.5 Résumé

Pour répondre à la question qui demandait l'évaluation des données probantes et des connaissances sur les meilleures pratiques pour prévenir et contrer les menaces à la sécurité publique, le comité d'experts s'est concentré sur les voies juridiques actuelles et potentielles qui pourraient s'appliquer au Canada. L'actuel tissu national de cadres juridiques — délits civils, droit criminel, droit civil du Québec, législation provinciale et fédérale sur la protection des renseignements personnels et autres instruments — donne aux individus, aux agents de l'État et aux organismes privés le pouvoir de s'attaquer aux comportements criminels et préjudiciables qui se produisent par le biais des TIC.

Ce tissu est toutefois complexe et se heurte à des difficultés découlant de l'arrivée de nouvelles TIC et de la modification des TIC existantes. D'une part, le droit criminel présente, selon certains, un angle mort lorsqu'il s'agit de prendre en compte l'expérience des femmes et des filles victimes et survivantes de violence cyberfacilitée. D'autre part, la capacité du CANAFE à prévenir la fraude et le blanchiment d'argent cyberfacilités est limitée par un manque de pouvoirs d'enquête et d'application de la loi. De plus, en raison de sa conception dépassée de la protection de la vie privée, le droit de la responsabilité délictuelle ne protège pas les participants d'une économie axée sur les données. De son côté, le droit relatif à la diffamation a eu du mal à s'adapter à la nature globale des activités en ligne et est mal outillé pour aborder la question de la responsabilité des intermédiaires sur Internet. Enfin, la coopération entre le secteur public et le secteur privé et l'absence de pouvoirs d'application de la loi constituent des défis pour le régime fédéral de protection des renseignements personnels applicable aux organisations du secteur privé. En somme, le comité d'experts a constaté que l'évolution technologique est un souci pour le droit public et le droit privé, ce qui a pour effet que les décideurs se demandent comment la réforme du droit national pourrait surmonter certains des problèmes que les TIC posent pour la sécurité publique au Canada.

Des propositions pour un meilleur recours au droit afin d'améliorer la santé globale de l'écosystème numérique ont été formulées dans le monde entier. L'Australie, l'Allemagne, la Nouvelle-Zélande, le Royaume-Uni, les États-Unis et l'Union européenne ont introduit ou adopté des lois visant à lutter contre la prolifération des crimes et méfaits cyberfacilités. Le comité d'experts a toutefois constaté qu'aucune de ces approches ne résout entièrement le problème. D'une part, les mesures visant à renforcer la surveillance réglementaire des espaces numériques (p. ex. les avis de retrait sanctionnés par l'État) ont conduit à une suppression excessive de contenu légal et suscité des inquiétudes quant à la liberté d'expression. D'autre part, l'absence d'intervention étatique dans le cadre de certains régimes d'immunité et de règles refuges confère aux entreprises privées

un pouvoir discrétionnaire sur la meilleure façon de contrôler le discours en ligne et peut conduire à une sous-réglementation des espaces numériques. Il est nécessaire de prendre en compte ces problèmes ainsi que les différences entre les systèmes juridiques et entre les cultures juridiques pour évaluer dans quelle mesure les méthodes suivies par d'autres pays conviennent au contexte canadien.

Si ce chapitre a donné un aperçu des lois et règlements actuels et proposés, l'*application* des lois concernant la cybercriminalité se heurte à une série d'obstacles supplémentaires, qui sont examinés au chapitre 6.

6

Difficultés et possibilités en matière d'application de la loi

Constatations du chapitre

- L'insuffisance des ressources au sein des forces de l'ordre et du système judiciaire dans son ensemble constitue un obstacle majeur à la rapidité des enquêtes et des poursuites en matière de crimes cyberfacilités.
- Le système de justice pénale n'est pas en mesure de faire efficacement face à la nature de plus en plus numérique de la criminalité, en raison de l'insuffisance des connaissances numériques générales et spécialisées aux stades de la prévention, de l'enquête et des poursuites.
- On dispose d'un ensemble d'outils numériques pour appuyer la prévention des crimes cyberfacilités et les enquêtes à leur sujet, mais chacun d'entre eux a des répercussions juridiques, sociétales et en matière de vie privée, qui doivent être évaluées et surveillées indépendamment avant, pendant et après leur utilisation.
- Une mauvaise communication au sein des forces de l'ordre et entre elles peut semer la confusion et entraîner l'exploitation inefficace des ressources.
- Les lacunes critiques en matière de données sur la fréquence et l'impact de la criminalité cyberfacilitée empêchent les forces de l'ordre et les gouvernements de relever ces défis et d'évaluer l'efficacité des interventions.

Le Canada fait face à des difficultés considérables dans l'application des cadres existants qui interdisent certains comportements préjudiciables se produisant en ligne. Cela signifie que, même dans les cas où il existe des lois ou des règlements qui permettent aux forces de l'ordre de répondre à ces méfaits, ces organismes sont souvent entravés dans leurs capacités à enquêter sur les actes criminels et à poursuivre leurs auteurs. Des services de police efficaces sont essentiels à la protection de la sécurité publique et des droits de la personne dans une société démocratique, et les exigences imposées à ces services au Canada ont considérablement augmenté. Les difficultés rencontrées par les forces de l'ordre dans l'application des lois contre les préjudices en ligne découlent principalement de la mésadaptation des structures et des méthodes actuelles à un environnement criminel que les technologies numériques ont radicalement transformé.

Ce chapitre commence par souligner les lacunes importantes de données et de connaissances sur la criminalité cyberfacilitée au Canada, qui rendent impossible une connaissance exacte des conséquences, une affectation efficace des ressources ou une évaluation significative des nouvelles mesures. Malgré les

graves lacunes dans les données, il est clair que les cas de crimes cyberfacilités sont en augmentation, qu'ils ne sont pas suffisamment signalés et qu'ils mettent à rude épreuve la capacité des forces de l'ordre canadiennes. La grave pénurie de compétences numériques spécialisées au sein des forces de l'ordre entraîne des retards considérables dans le traitement des preuves numériques. Dans le même temps, en raison de leur manque de compétences numériques de base, il est difficile pour les agents généralistes d'intervenir face aux crimes cyberfacilités. La pénurie de spécialistes est en partie due aux problèmes systémiques créés par la structure organisationnelle désuète des forces de l'ordre au Canada et à la résistance au changement, malgré les rôles élargis que l'on attend des policiers. Face à ces problèmes, le comité d'experts examine les possibilités de moderniser les forces de l'ordre par une professionnalisation accrue, une meilleure formation au numérique et la coordination entre les organismes.

Le chapitre examine ensuite les écueils auxquels se heurtent les enquêtes criminelles, en commençant par décrire les difficultés que les forces de l'ordre ont à accéder aux preuves numériques. Le comité d'experts étudie les possibilités et les facteurs liés au traitement des données, à la détection numérique et à la déclaration en ligne avant de passer à un examen approfondi des avantages et des risques apportés par l'intelligence artificielle (IA). Par exemple, les violations résultant de l'utilisation de la technologie de reconnaissance faciale (TRF) par les forces de l'ordre ont été prédites par de nombreux experts et illustrent les risques notables du déploiement de nouvelles technologies sans orientation, transparence et responsabilité appropriées. Le comité d'experts souligne la nécessité pour les forces de l'ordre de disposer de directives claires sur les outils et les approches qu'elles emploient, ainsi que d'effectuer une évaluation indépendante avant le déploiement de nouvelles technologies et une surveillance continue pour garantir la protection des droits de la personne et de la vie privée. Enfin, le comité d'experts décrit brièvement les défis posés par les contraintes de capacité dans l'ensemble du système de justice pénale, y compris au sein du système judiciaire, qui sont particulièrement dommageables étant donné les délais constitutionnels pour juger les affaires criminelles.

Le comité estime que les difficultés auxquelles font face les forces de l'ordre canadiennes devant la prolifération de la criminalité cyberfacilitée sont considérables et ne feront qu'augmenter à mesure que les auteurs de cybermenaces trouveront de nouvelles façons d'utiliser la technologie comme outil pour infliger des dommages. Ces difficultés exigent que les forces de l'ordre améliorent leurs démarches de prévention, d'enquête et de poursuite relatives aux crimes cyberfacilités. Le recours à des outils numériques conformes aux exigences de respect de la vie privée et des droits de la personne peut aider les forces de l'ordre à assurer la sécurité publique contre les acteurs malveillants.

6.1 Lacunes de données

Les données sont insuffisantes pour évaluer la fréquence et les répercussions de la cybercriminalité au Canada

Jusqu'à présent, les meilleures données pancanadiennes, recueillies et conservées par Statistique Canada, ont été extrêmement insuffisantes pour plusieurs raisons, notamment des définitions et des déclarations non uniformes entre les ministères (chapitre 1). Cette lacune se traduit de manière critique par un manque de données fiables et cohérentes sur la cybercriminalité; elle empêche les corps policiers de comprendre toute l'étendue du problème et d'employer les meilleures stratégies d'intervention et de prévention face à la cybercriminalité (Dupont, 2021). Des changements dans la façon de signaler les cybercrimes au Canada pourraient permettre de résoudre partiellement ce problème (StatCan, 2021c). On a d'ailleurs annoncé que les corps policiers de tout le pays devront catégoriser les actes criminels cyberassistés et cyberfacilités au moyen du Compendium nord-américain sur la classification de la cybercriminalité (NACCC) et partager ces données avec Statistique Canada (section 1.3.2).

Les limitations des données s'étendent à la composition des unités policières et aux lacunes particulières en matière de capacités auxquelles elles sont confrontées. Par exemple, il est difficile de déterminer le nombre de spécialistes en criminalistique numérique au Canada, car les corps policiers et Statistique Canada ne recueillent pas cette information de façon systématique et uniforme (Dupont, 2021).

L'augmentation de la fréquence des enquêtes sur les personnes victimes de cybercrime au Canada (à l'image de ce qui se fait dans d'autres pays, comme le Royaume-Uni) pourrait faciliter la planification et la mise en œuvre de mesures efficaces contre la cybercriminalité (Dupont, 2021). Ces enquêtes sont utiles pour orienter les ressources vers l'aide aux victimes et aux survivants de crimes cyberfacilités, mais elles permettent également de définir des approches visant à prévenir les préjudices. En particulier, la mise à jour régulière des statistiques sur les personnes victimes de cybercrime serait particulièrement utile pour les crimes chroniquement sous-déclarés, car des renseignements limités sur la fréquence et les effets peuvent être glanés à partir des statistiques sur les crimes signalés par la police. En outre, des statistiques fiables et des recherches qui mesurent à la fois la prévalence de la cybercriminalité et ses conséquences directes et indirectes sur les individus aideraient à l'élaboration, à la mise en œuvre et à l'évaluation de stratégies pour la combattre (Dupont, 2021). Tant que des comptes rendus statistiques fiables, cohérents et efficaces n'auront pas été conçus, il sera difficile pour les gouvernements au Canada de déterminer où se situent les problèmes, où des mesures sont prises pour lutter contre les activités illégales ou préjudiciables et où des ressources supplémentaires pourraient être nécessaires.

Le manque de données minimise l'ampleur des effets de la cybercriminalité et empêche une évaluation efficace des interventions

De l'avis du comité d'experts, les lacunes importantes dans les données relatives à la criminalité cyberfacilitée au Canada peuvent donner l'illusion que ses répercussions ne sont pas graves ou répandues, malgré le nombre croissant de données probantes qualitatives ou anecdotiques qui indiquent le contraire. Il est également difficile de diriger avec exactitude les ressources et les actions là où elles pourraient avoir le plus d'effet, simplement parce que les domaines qui ont le plus besoin de ressources ne sont pas toujours immédiatement visibles. À l'avenir, les nouvelles politiques, approches ou technologies mises en œuvre pour renforcer la sécurité publique seront plus avantageuses si elles sont accompagnées d'une rigoureuse recension publique des méfaits et des crimes en ligne et si elles peuvent soutenir une recherche de haute qualité, ce qui fait actuellement défaut dans le domaine policier au Canada. L'évaluation implique en partie l'établissement d'une base de référence, ce qui est actuellement impossible en raison de la rareté des données sur la criminalité cyberfacilitée et à son impact au Canada. Combler les lacunes et favoriser une évaluation rigoureuse présenteraient des avantages notables pour les décideurs politiques et les spécialistes de l'application de la loi, en leur permettant notamment de mieux comprendre et résoudre les problèmes, de diriger les ressources et de développer les nouvelles initiatives les plus efficaces.

6.2 Structure et dotation en personnel

6.2.1 Compétences numériques spécialisées et élémentaires

Il y a une pénurie d'expertise et de ressources spécialisées nécessaires pour analyser les preuves numériques

Ces dernières décennies, le maintien de l'ordre est devenu plus complexe et progressivement plus exigeant pour diverses raisons, notamment la prolifération de la cybercriminalité (Leuprecht, 2019) et les décisions judiciaires qui obligent les agents à suivre des procédures d'enquête considérées comme compliquées ou longues (p. ex. l'accès aux renseignements de base sur les abonnés, abordé à la section 6.3.1). Dans le même temps, les ressources pour enquêter sur les crimes cyberfacilités, y compris l'expertise et les moyens techniques les plus récents, se raréfient (Dupont, 2021). Si l'insuffisance des capacités a des conséquences concrètes pour tous les types de crimes, le problème peut être particulièrement aigu pour les crimes cyberfacilités (ou d'autres crimes comportant des cyberéléments importants).

Les preuves numériques présentent plusieurs caractéristiques qui les distinguent des preuves physiques. Elles ont fréquemment une portée plus large, peuvent être plus sensibles sur le plan personnel, sont généralement mobiles et nécessitent une formation, une expertise et des outils différents (Goodison *et al.*, 2015). Les enquêtes portent souvent sur plusieurs appareils électroniques (p. ex. des ordinateurs portables, des téléphones intelligents, des dispositifs GPS), qui peuvent contenir des preuves numériques pertinentes, chacun utilisant une infrastructure et un système d'exploitation différents (Vincze, 2016). Il est peu probable qu'un seul enquêteur ait les connaissances spécialisées nécessaires pour examiner chaque dispositif concerné, ce qui signifie que plusieurs enquêteurs doivent travailler en collaboration, ce qui étire les capacités en personnel (Vincze, 2016).

Même si les outils technologiques nécessaires à l'analyse et au traitement des preuves numériques sont disponibles, les opérations policières spécialisées requièrent souvent un important travail manuel. Par exemple, des outils sophistiqués de recherche dans les bases de données peuvent réduire le nombre de correspondances possibles pour un auteur de crime, mais la recherche de correspondance finale est effectuée par les policiers eux-mêmes au moyen de longues évaluations manuelles (Watson et Huey, 2020). Certaines des possibilités technologiques examinées à la section 6.3.3 réduiront la demande de main-d'œuvre, mais elles ne résoudront pas le problème de l'insuffisance des capacités en général, car il y a une pénurie de personnel possédant l'expertise numérique nécessaire pour occuper des postes propres à la cybersécurité. Le problème est en partie dû à la structure paramilitaire de la police décrite à la section 6.2.2.

Les contraintes de capacité ont entraîné des arriérés de preuves numériques

La forte prévalence de la cybercriminalité et le besoin d'une expertise spécialisée ont poussé à la création ou à l'expansion d'unités policières spécialisées, dont les délais de traitement sont souvent longs à cause de l'insuffisance des ressources, du nombre croissant de demandes d'assistance technique et des grandes quantités de données et d'appareils saisis au cours des enquêtes (Baril, 2014; Dupont, 2021). Ces arriérés de preuves numériques sont aggravés par le manque d'équipement (Goodison *et al.*, 2015). Le problème se pose dans de nombreux pays.

En Angleterre et au Pays de Galles, par exemple, en mars 2022, plus de 12 000 appareils numériques attendaient d'être examinés dans 32 corps policiers (ITV News, 2020). Simon Kempton, responsable de la technologie à la Fédération des polices d'Angleterre et du Pays de Galles, a expliqué que les enquêteurs étaient « submergés » par les preuves numériques. Il a également constaté que « le plus gros problème de l'accumulation de dispositifs est qu'il en résulte des problèmes de communication, certains éléments de preuve potentiellement vitaux n'arrivant

pas à temps au tribunal » [traduction libre] (ITV News, 2020). Bien qu'il n'ait pas été possible de trouver des données sur les arriérés au Canada, des problèmes similaires existent au niveau national, d'après l'expérience des membres du comité d'experts.

Il existe une pénurie de compétences numériques élémentaires au sein des forces de l'ordre

Outre l'insuffisance de personnel dans des rôles spécialisés, les forces de l'ordre manquent largement des compétences numériques générales nécessaires pour faire face à la criminalité cyberfacilitée. Une étude a révélé que plus de 60 % des agents de police en Angleterre et au Pays de Galles ne se sentaient pas prêts à répondre aux incidents de cybercriminalité (Burruss *et al.*, 2020). Dans le même ordre d'idées, une enquête menée auprès d'agents de patrouille aux États-Unis a révélé que la plupart d'entre eux estimaient que les forces de l'ordre locales ne devraient pas être les principaux intervenants lors d'incidents de cybercriminalité, qui seraient mieux traités par des unités spécialisées (Bossler et Holt, 2012); des résultats similaires ont été rapportés en Australie (Cross *et al.*, 2021). En outre, le niveau général de connaissance des caractéristiques de la cybercriminalité et de la manière de préserver les preuves numériques est faible (Dupont, 2021). Ces déficits de compétences peuvent avoir une incidence sur la manière dont les agents répondent aux signalements de crimes cyberfacilités. Une étude s'appuyant sur une enquête menée auprès de policiers en Angleterre et au Pays de Galles a révélé que, bien que la plupart des agents soient exposés à des incidents de cybercriminalité, ils consacrent une proportion relativement faible de leurs heures de travail à y répondre par rapport à d'autres types de crimes (Holt *et al.*, 2019). Même si des données équivalentes ne sont pas disponibles au Canada, des tendances similaires ont été observées (Dupont, 2021).

L'augmentation des fonds destinés à améliorer la cybersécurité au Canada n'a pas été dirigée vers les services de police locaux

Dupont (2021) soutient que le plus grand défi de la lutte contre la criminalité cyberfacilitée au Canada (p. ex. l'exploitation en ligne) est le manque de moyens pour traiter le volume même des incidents qui se produisent. Comme nous l'avons vu au chapitre 3, la majorité de ces crimes sont commis au Canada, ce qui signifie qu'ils relèvent de la compétence des forces de l'ordre locales (y compris de la GRC). Il convient de noter que, bien que l'amélioration de la cybersécurité du Canada ait été abordée dans le budget fédéral de 2022, la grande majorité des nouveaux fonds (875,2 millions de dollars sur 5 ans) a

été affectée au Centre de la sécurité des télécommunications (CST)[18]. Aucun financement dans le cadre de cette initiative n'a été octroyé à Sécurité publique Canada ou à la GRC (GC, 2022b).

6.2.2 Recrutement et rétention des spécialistes

La structure paramilitaire des services de police au Canada ne se prête pas à la rétention des compétences spécialisées nécessaires pour enquêter sur les crimes cyberfacilités

Au Canada, la plupart des services de police suivent un modèle paramilitaire qui comprend une structure de grades rigide et une formation de base commune (Fry et Berkes, 1983; SECU, 2021). Les recrues entrent généralement dans cette structure paramilitaire au bas de la hiérarchie policière, après une formation initiale axée sur l'intervention rapide et la patrouille, indépendamment des besoins particuliers d'un corps de police donné. Si les agents peuvent arriver dans un corps avec des compétences numériques spécialisées, ou acquérir ces compétences sur le tas, le système de promotion n'incite pas au développement des compétences. Comme l'explique le CAC (2014), le système actuel « privilégie la promotion en fonction de l'ancienneté aux dépens de la spécialisation et du développement de l'expertise ». En outre, le comité d'experts note que lorsqu'il reçoit une promotion et monte en grade, un agent qui a acquis des compétences numériques spécialisées se retrouve souvent dans une division où il ne pourra pas appliquer ces compétences ou les perfectionner.

Les problèmes créés par l'avancement hiérarchique au sein des forces de l'ordre ne sont pas uniques au Canada. Certains services de police prennent toutefois des mesures pour encourager l'acquisition de compétences et la formation continue. Par exemple, en France, la gendarmerie nationale[19] a lancé en 2018 un programme qui soutient les officiers de gendarmerie souhaitant poursuivre un doctorat (CGE, 2022). Ce soutien porte sur les frais de scolarité, l'octroi de jours de congé et l'orientation (p. ex. la détection de superviseurs potentiels ou la mise en relation avec des experts du monde des affaires). Une fois leur diplôme obtenu, les gendarmes reçoivent une épinglette spéciale à arborer sur leur uniforme, ce qui reflète la volonté de la gendarmerie de mettre en valeur et de récompenser la formation continue (Ministère de l'Intérieur, 2019).

18 Une petite partie des nouveaux fonds a été affectée à l'élargissement « de la protection de la cybersécurité pour les petits ministères, les organismes et les sociétés d'État » (GC, 2022b).

19 La *gendarmerie nationale* est une branche des forces armées françaises qui est responsable du maintien de l'ordre dans les régions rurales de France (Terrill, 2013).

La perception interne de la cybercriminalité et du rôle des spécialistes du numérique peut avoir une incidence sur les capacités

Le manque de reconnaissance des cyberspécialistes travaillant dans l'écosystème policier, associé à leur faible visibilité, peut également contribuer aux contraintes de capacité ou les accroître. Une étude a révélé que le travail des policiers canadiens dans les unités de lutte contre l'exploitation des enfants sur Internet n'est pas toujours reconnu comme un « travail de police », ce qui peut amener les enquêteurs à éprouver un sentiment d'aliénation, du cynisme et une faible satisfaction professionnelle (Spencer *et al.*, 2020). Une autre étude menée en Australie a révélé que les spécialistes des unités de lutte contre la cybercriminalité estiment qu'ils ne bénéficient pas de ressources adéquates ou de la reconnaissance de leur travail, ce qui a un impact négatif sur le recrutement (Harkin et Whelan, 2019). Les expériences négatives du personnel découlent, en partie, du fait que la haute direction, les superviseurs et les policiers d'autres unités ont souvent une faible connaissance de la nature du travail et des besoins des unités de cyberpolice; cela a des répercussions correspondantes sur le désir de rester de ces spécialistes, tout comme sur l'engagement organisationnel général à investir dans la formation continue en cybernétique (Harkin *et al.*, 2018).

Le fait que la criminalité cyberfacilitée évolue au sein d'une hiérarchie informelle d'activités criminelles influence à la fois la perception de la police et la façon dont elle réagit lorsque ces activités sont signalées (Dupont, 2021). Une étude australienne reposant sur des entrevues a révélé que les forces de l'ordre peuvent minimiser les méfaits de la violence conjugale en ligne, du cybertraquage et du cyberharcèlement (Powell et Henry, 2018). Cette réaction peut être due en partie au fait que les agents d'application de la loi ont l'impression de ne pas posséder les compétences nécessaires pour répondre efficacement à la criminalité cyberfacilitée (Dupont, 2021). La reconnaissance de la cyberfraude par la police, par exemple, est importante pour les victimes, car elle peut valider leurs préoccupations, encourager le signalement et contribuer à atténuer le sentiment de honte (Cross et Blackshaw, 2015).

La civilianisation des forces de l'ordre progresse, mais les salaires des employés possédant des compétences numériques spécialisées devront être comparables, voire supérieurs, à ceux des agents en uniforme

La *civilianisation* fait référence à l'utilisation d'employés civils (c.-à-d. de non-agents) au sein des forces de police pour effectuer certaines tâches. En théorie, elle permet aux agents de se concentrer sur les volets de l'application de la loi qu'ils sont les seuls à pouvoir exécuter (Kostelac, 2008). Le CAC (2014) a constaté que la proportion de civils travaillant dans les corps policiers par rapport aux

agents était en hausse au Canada, bien qu'on en sache peu sur les postes exacts qu'ils occupent. Cela dit, les unités canadiennes de lutte contre la cybercriminalité ont commencé à ouvrir certains de leurs postes aux civils. En 2019, la Police provinciale de l'Ontario (OPP) a ouvert un centre de cyberopérations qui comprend une équipe d'enquêtes sur la cybercriminalité, une équipe de criminalistique numérique et une unité judiciaire d'analyse vidéo dotées d'une combinaison d'agents en uniforme, d'agents spéciaux et de civils possédant une expertise technique (Goldfinger, 2019). De même, en 2021, la GRC a annoncé qu'elle allait également intégrer 35 enquêteurs civils dans ses activités (Northcott, 2021).

Deux des avantages cités de l'embauche de personnel civil — ils sont moins payés que les agents et peuvent acquérir une expertise stable dans un corps (CAC, 2014) — ne s'appliquent pas aux civils ayant des compétences numériques avancées. Pour attirer du personnel hautement qualifié à travailler dans le domaine de la criminalistique numérique, il faudra peut-être que les salaires et les avantages sociaux soient comparables à ceux des agents (Kiedrowski *et al.*, 2015), tandis que les spécialistes entièrement qualifiés peuvent exiger des salaires encore plus élevés pour concurrencer les salaires du privé (Dupont, 2021). Si, en théorie, le manque de promotion permet de maintenir l'expertise en place, l'absence de toute possibilité d'avancement dans les postes civils peut pousser les spécialistes à quitter les organismes policiers après quelques années, en particulier si leur salaire est considérablement inférieur à ceux du secteur privé. Par conséquent, la création de postes civils qui ne sont pas concurrentiels par rapport à d'autres postes du secteur public ou privé peut entraîner des difficultés de recrutement et un fort taux de roulement du personnel, avec pour effet que la civilianisation des forces de l'ordre pourrait ne pas améliorer la pénurie actuelle de compétences numériques spécialisées. La professionnalisation accrue des services de police au Canada (section 6.2.4) pourrait donc se révéler plus efficace pour garantir une capacité soutenue de spécialistes du numérique dans les corps policiers.

6.2.3 Coopération et coordination

Il existe des problèmes de coopération à l'intérieur des corps policiers et entre eux

Au Canada, un éventail de forces de l'ordre sont chargées de différents territoires et, dans certains cas, de différentes activités criminelles (StatCan, 2020b). La coordination entre ces organismes est particulièrement importante pour les crimes qui se produisent sur plusieurs territoires, comme c'est souvent le cas des crimes cyberfacilités. Dans ces types de crimes, la victime et l'auteur peuvent être situés physiquement sur des territoires différents, et les preuves numériques sont

souvent hébergées par un fournisseur de services international (p. ex. les platesformes de médias sociaux) (Powell et Henry, 2018). De plus, alors que la criminalité cyberfacilitée est fortement mondialisée, les organisations policières sont souvent organisées localement, ce qui rend difficile l'adaptation de leurs tactiques d'intervention (Dupont, 2021).

Le manque de coordination et de compréhension mutuelle au sujet des renseignements pouvant être partagés entre les forces de l'ordre et de renseignement au Canada est préoccupant (OSSNR, 2019a; Carvin *et al.*, 2021b). Bien qu'il existe de nombreux cas où la circulation de l'information entre les organismes de renseignement devrait être limitée, un examen de la Direction de la sécurité interne du SCRS a révélé que ce dernier ne possédait pas de politique et de procédure claires sur la façon et le moment où il peut et doit signaler et partager des renseignements avec les forces de l'ordre (p. ex. une activité criminelle présumée découverte au cours d'une évaluation de sécurité) (OSSNR, 2019b). D'après l'analyse d'un cas, il y avait des retards dans le partage des renseignements (OSSNR, 2019b). Une autre étude a constaté que certains obstacles à la coopération entre le SCRS et la GRC sont dus à des systèmes de communication interorganismes incompatibles ou non sécurisés, ainsi qu'à la résistance au dévoilement des sources et des méthodes du SCRS dans les poursuites criminelles (OSSNR, 2019a). Il en résulte une sous-utilisation des renseignements provenant du SCRS dans les enquêtes de la GRC (OSSNR, 2019a), ce qui peut nuire aux efforts de lutte contre la cybercriminalité au Canada. Il existe également des problèmes de coordination entre les différentes unités d'un même corps — un problème qui n'est pas propre au Canada. Les unités policières spécialisées chargées de diverses mesures d'enquête sur la cybercriminalité (p. ex. criminalistique, interception des communications électroniques, cyberattaques) ne sont pas toujours bien intégrées aux efforts des policiers de première ligne ou des procureurs pénaux locaux (Goodison *et al.*, 2015; Dupont, 2021).

6.2.4 Possibilités de modernisation des forces de l'ordre

La professionnalisation du maintien de l'ordre pourrait favoriser l'acquisition de compétences numériques spécialisées, mais la normalisation de la formation aux compétences numériques reste difficile à réaliser

Au Canada, les agents de police assument un éventail de rôles différents, chacun d'eux exigeant des compétences particulières; cela dit, certains des agents peuvent ne pas être suffisamment formés pour y parvenir. Il s'agit notamment de s'attaquer au problème croissant du crime cyberfacilité, qui nécessite des compétences numériques spécialisées non requises pour les crimes exclusivement non numériques (Dupont, 2021). Des appels ont été lancés afin que les forces de

police s'orientent vers une professionnalisation accrue pour diverses raisons, notamment pour permettre la différenciation des rôles au sein des forces de l'ordre et une moindre dépendance à l'égard des policiers généralistes (CAC, 2014). Les généralistes seront toujours nécessaires, notamment pour les interventions, mais la différenciation permettrait aux agents de se spécialiser dans un domaine particulier et d'y rester, même s'ils sont promus.

La professionnalisation peut inclure un agrément officiel, tel que la standardisation et la qualification, qui enlève une partie de la charge de formation des forces de l'ordre elles-mêmes (CAC, 2014). La standardisation crée également une uniformité entre les forces de l'ordre et favorise la responsabilité et la légitimité. Comme dans de nombreuses autres professions, le perfectionnement professionnel continu peut être lié à la fois à l'agrément et à l'avancement, ce qui garantit que les employés sont encouragés à développer leurs compétences et récompensés quand ils le font (CAC, 2014).

Une question centrale est de savoir comment professionnaliser la formation numérique des corps policiers étant donné le manque de standardisation entre les établissements de formation policière, les universités et les collèges (Goodison *et al.*, 2015; Dupont, 2021). Par exemple, le baccalauréat technologique en informatique judiciaire de deux ans de l'Institut de technologie de la Colombie-Britannique comporte des cours sur la criminalistique numérique, la cybersécurité, les preuves légales et la sécurité des réseaux, entre autres. La plupart de ces cours peuvent également être suivis individuellement à des fins de perfectionnement professionnel (BCIT, s.d.). En comparaison, le certificat en cybersécurité, protection des données et criminalistique numérique de l'Université métropolitaine de Toronto comprend six cours obligatoires (en sécurité des réseaux et en informatique judiciaire, entre autres) et peut être obtenu en un an (TMU, 2022). Dans l'ensemble, il existe des possibilités pour le secteur de l'enseignement supérieur canadien d'offrir une formation spécialisée dans le cadre de diplômes, de grades ou de cours uniques adaptés aux employés des forces de l'ordre.

Cependant, tous les services de police ne sont pas en mesure d'envoyer des agents dans des établissements d'enseignement postsecondaire, et même lorsqu'ils le peuvent, le manque de standardisation peut créer des lacunes dans certaines matières enseignées (Stigall et Choo, 2021). Actuellement, il n'y a pas suffisamment de formation proposée dans des domaines spécifiques, notamment sur la cyberlégalité propre au Canada, les cryptomonnaies, la prévention de la cybercriminalité, l'aide aux victimes et la criminalistique numérique et de réseau (Beesley, 2021). La standardisation n'est cependant pas un exercice simple, et les efforts passés pour harmoniser la formation cybernétique à l'échelle internationale (p. ex. par le biais de l'Organisation internationale sur la preuve informatique) n'ont pas été couronnés de succès (Dupont, 2021).

Le secteur privé a la possibilité de jouer un plus grand rôle dans le traitement des preuves numériques et dans le soutien à la formation

Certaines forces de l'ordre ont déterminé que leurs capacités de formation interne sont insuffisantes pour assurer la formation aux compétences numériques spécialisées. Au Royaume-Uni, par exemple, His Majesty's Inspectorate of Constabulary (HMIC, l'Inspection de la gendarmerie et des services d'incendie et de sauvetage de Sa Majesté) a constaté que le College of Policing ne peut pas fournir une formation spécialisée perfectionnée; ces compétences doivent donc être inculquées avec l'aide de partenaires externes (HMIC, 2015). Le HMIC note plusieurs avantages à faire appel à des fournisseurs de formation tiers, notamment ne pas avoir à maintenir une infrastructure de formation, réduire les coûts de conception des programmes et permettre aux forces de l'ordre de « bénéficier des connaissances du secteur privé » [traduction libre] (HMIC, 2015).

Une autre proposition britannique, qui verrait de la même manière le secteur public apprendre du secteur privé, consisterait à détacher des agents des forces de l'ordre afin d'effectuer un transfert de connaissances entre la police et le secteur privé (Hitchcock *et al.*, 2017). Selon ce modèle, des policiers spécialisés (ou d'autres employés de la police) pourraient être envoyés travailler dans des entreprises technologiques pendant quelques mois, afin d'acquérir de nouvelles compétences numériques. Il existe toutefois un risque que certaines entreprises technologiques soient réticentes à de tels détachements (et à de telles relations). En outre, la collaboration croissante entre le secteur public et le secteur privé sur les questions de sécurité et de surveillance demande de fixer des exigences strictes en matière de rapports, une évaluation des risques et des évaluations fréquentes de la relation afin de garantir la protection de la vie privée.

Au-delà de la formation, le comité d'experts estime qu'il existe des possibilités de collaboration entre les forces de l'ordre et le secteur privé pour l'exécution de tâches précises nécessitant de l'équipement et des compétences hautement spécialisés. Ces partenariats pourraient exploiter le rôle important que le secteur privé joue déjà dans la sécurité numérique. Par exemple, des organisations privées pourraient être chargées de retracer et de saisir des cryptomonnaies ou de procéder à l'analyse judiciaire de réseaux. Tirer parti de la capacité du secteur privé à effectuer ces tâches chronophages pourrait libérer du temps et des ressources pour la police. Cependant, ces partenariats devront être mis en œuvre avec prudence, afin de préserver l'indépendance et l'intégrité des enquêtes de police et des éventuelles poursuites criminelles.

Inculquer des connaissances numériques générales à l'ensemble des agents améliorerait la capacité des forces de l'ordre à enquêter sur les cybercrimes

Inculquer les connaissances numériques générales à plus de personnel ne vise pas à faire de tous les agents des experts en technologie. Le but est plutôt l'acquisition de nouvelles compétences numériques qui facilitent un éventail de travaux policiers, puisque « les informations numériques peuvent enrichir [...] les enquêtes criminelles » [traduction libre] (Leukfeldt *et al.*, 2013). De plus, cette formation peut aider les agents ayant peu d'expérience en matière de cybercriminalité à surmonter leur hésitation à traiter des cas de crime cyberfacilité. L'utilisation de platesformes en ligne peut rendre cette formation accessible à tous les agents à un coût modéré (Dupont, 2021).

Ce type de formation est déjà utilisé au Canada et ailleurs (Dupont, 2021). En France, le programme de formation de la gendarmerie nationale a été mis à jour pour refléter l'importance croissante des compétences numériques, avec le lancement d'un programme pilote qui accroît considérablement les volets numériques dans la formation de base (Hours, 2022). La gendarmerie explique que le cours ne vise pas à former des spécialistes, mais plutôt à introduire davantage de connaissances et une meilleure compréhension du numérique dans tous les services. De même, en Suisse, l'Institut Suisse de Police a conçu la formation E-CC (apprentissage en ligne sur le cybercrime) afin de diffuser rapidement une formation d'initiation aux 20 000 policiers du pays. La formation est offerte dans les trois langues officielles de la Suisse et est également accessible à certains employés civils (Brugoni, 2018).

Au Canada, le projet Formation en cybercriminalité et développement des compétences numériques pour les forces de l'ordre canadiennes du Réseau canadien du savoir policier (RCSP) s'efforce de fournir ce type de formation à tous les agents (RCSP, 2021). Le projet a débuté par la détermination de dix compétences numériques concernant les preuves numériques, les cybercrimes et les crimes cyberfacilités, ainsi que différents rôles occupés au sein des forces de l'ordre (p. ex. premier intervenant, analyste en cybercriminalité) (Beesley, 2021). On a ensuite créé une matrice prenant en compte le niveau de compétence requis pour les personnes assumant divers rôles. Par exemple, les premiers intervenants ont besoin de faibles compétences en cryptomonnaies et en chaîne de blocs, tandis que le niveau de compétence des analystes en cybercriminalité dans ce domaine doit être élevé.

Une analyse a ensuite révélé des lacunes importantes en matière de formation pour les rôles de maintien de l'ordre généraliste (Beesley, 2021). Les groupes de discussion composés de « praticiens et d'experts en lutte contre la cybercriminalité issus de l'industrie et des services de police de tout le Canada »

[traduction libre] étaient largement d'accord pour dire qu'une formation supplémentaire sur la cybercriminalité était nécessaire et que cette formation était « requise à tous les niveaux, du niveau élémentaire au niveau avancé » [traduction libre] (Beesley, 2021). Le RCSP travaille actuellement avec des experts à l'élaboration d'un programme de formation généraliste, dans les deux langues officielles, destiné aux travailleurs de première ligne (RCSP, 2021).

Toutefois, l'élaboration de programmes de formation ou de cours prend du temps et il peut être difficile de suivre le rythme de l'évolution technologique. Comme pour les formations axées sur des compétences spécialisées, il existe des possibilités de partenariat avec le secteur privé ou avec les établissements universitaires pour concevoir et dispenser des cours sur les compétences numériques de base utiles à tous les agents des forces de l'ordre. Cependant, même lorsque la formation est accessible, elle peut ne pas être utilisée à son plein potentiel. Le catalogue du RCSP propose plusieurs cours en ligne relatifs à la cybercriminalité[20], mais l'inscription n'est pas obligatoire et il appartient aux corps policiers ou aux agents à titre individuel de décider s'ils veulent les suivre (Dupont, 2021). En outre, la plupart des cours ne sont pas gratuits (bien qu'ils soient peu coûteux) et beaucoup ne sont offerts qu'en anglais (RCSP, 2022). Il en résulte que, bien que le Canada dispose d'une méthode prometteuse de formation des agents, la formation n'est pas suivie par tous les agents qui pourraient en bénéficier, ou ne leur est pas accessible.

Les organes de coordination peuvent faciliter l'allocation des ressources et éviter le dédoublement des efforts

Conscients que les ressources sont limitées, plusieurs pays ont mis sur pied des organes de coordination qui facilitent la mise en commun des ressources et tentent d'éviter le dédoublement des efforts. Ces organes peuvent également favoriser la collaboration avec les forces de l'ordre internationales, ce qui est particulièrement important étant donné que la criminalité en ligne traverse souvent les frontières. La Convention de Budapest (encadré 5.4) fournit un cadre promouvant les initiatives de coordination internationale.

La structure et le mandat exacts des organes de coordination varient selon l'État. Le National Cyber Crime Network (réseau national de lutte contre la cybercriminalité) au Royaume-Uni en est un exemple. Créé dans le cadre de la Stratégie nationale de cybersécurité de 2016–2021 (Gouv. du Royaume-Uni, 2021c), il comprend plusieurs unités, chacune ayant son propre rôle. La National Cyber Crime Unit (Unité nationale de lutte contre la cybercriminalité) de la National Crime Agency (Agence nationale contre le crime) assure la direction et la

20 Le catalogue de cours du RCSP contient des cours courts élaborés par d'autres fournisseurs de contenu, comme les services de police municipaux, la GRC et des organismes à but non lucratif (RCSP, 2022).

coordination, tandis que les unités régionales et locales de lutte contre la cybercriminalité sont chargées d'enquêter sur les infractions et d'aider les communautés locales à se protéger contre la cybercriminalité. Action Fraud (hébergé par la police municipale de Londres) est chargé de l'analyse et du triage à partir des rapports de criminalité centralisés. Il transmet les crimes jugés particulièrement graves ou complexes à la National Crime Agency ou aux réseaux régionaux, tandis que tous les autres cas sont confiés aux corps locaux (Gouv. du Royaume-Uni, 2021c). En plus d'éviter le dédoublement des efforts, un organe de coordination centralisé peut garantir que les crimes les plus graves sont examinés par les équipes les plus compétentes, libérant ainsi les autres équipes pour qu'elles puissent enquêter sur d'autres cybercrimes.

Au Canada, le Groupe national de coordination contre cybercriminalité (GNCC) joue un rôle de coordination depuis qu'il a atteint sa capacité opérationnelle en avril 2020 (GRC, 2021d). Composé d'agents de la GRC et de civils, le GNCC devrait atteindre sa pleine capacité en 2024 (GRC, 2021d). Il s'agit d'un système en trois parties géré par la GRC (2020c) dans le but « de réduire la menace, les répercussions et le nombre de victimes de la cybercriminalité au Canada » (GRC, 2021d). Le GNCC devrait comprendre un site Web de signalement public, qui permettra aux particuliers et aux entreprises de signaler des cybercrimes tels que l'utilisation de logiciels malveillants, le piratage, la cyberfraude, le vol d'identité, la falsification et l'extorsion (GRC, 2020c). À partir de là, les rapports seront collectés par la solution interne du GNCC, un dépôt de données centralisé dans lequel les nouveaux rapports seront analysés et comparés à une base de données afin de définir les rapports sur des cybercrimes, les incidents et les enquêtes en cours potentiellement liés. L'objectif du GNCC est de mettre en relation les enquêteurs en cybercrimes de toutes les provinces et de tous les territoires et de fournir les outils et le soutien nécessaires au recueil, à l'analyse et au partage des données et des renseignements par le portail de la police et de ses partenaires. En raison de la nature potentiellement sensible des données contenues dans la base de données de la solution interne du GNCC, l'accès y est soigneusement contrôlé et accordé de façon sélective aux forces de l'ordre et à leurs partenaires de sécurité autorisés (GRC, 2020c).

Le GNCC a déjà connu un certain succès. Avec d'autres partenaires canadiens, il a travaillé avec Europol à l'opération GoldDust (Ville de Calgary, 2021). Cette opération visait l'entreprise de rançongiciel REvil, qui vendait des logiciels malveillants à des clients, lesquels les utilisaient ensuite pour lancer des attaques consistant à chiffrer ou à voler des données, puis à extorquer de l'argent en échange de ces données. Les enquêteurs ont estimé qu'environ 600 infections (sur 7 000 dans le monde) utilisant ce logiciel malveillant se sont produites au Canada. L'enquête canadienne a cerné des infrastructures au Canada, ainsi que des

infrastructures et des suspects dans de nombreux pays d'Europe et d'Asie. Les suspects sont poursuivis aux États-Unis et dans des pays de l'Union européenne (Ville de Calgary, 2021).

6.3 Enquêtes criminelles

6.3.1 Accès aux preuves numériques

Les preuves numériques constituent souvent un élément essentiel des enquêtes de police

Les communications numériques, sous une forme ou une autre, sont utilisées dans la plupart des actes criminels. Par conséquent, les renseignements numériques font souvent partie intégrante des preuves nécessaires aux enquêtes et aux poursuites judiciaires. Cela signifie que les forces de l'ordre doivent être en mesure de travailler avec des preuves provenant d'espaces numériques afin d'être plus efficaces. Devant l'importance croissante des preuves numériques, certaines modifications ont été apportées aux cadres juridiques, principalement la *Loi sur la protection des Canadiens contre la cybercriminalité*, qui prévoit des outils d'enquête spécialisés pouvant être employés pour obtenir des preuves numériques ainsi que des sanctions pour les fournisseurs de services qui ne s'y conforment pas (GC, 2014). Ces outils comprennent des modifications des règles relatives aux mandats de perquisition et aux ordonnances de communication en ce qui a trait aux preuves numériques, ainsi que des exigences de préservation pour empêcher la suppression de preuves électroniques. Le ministère de la Justice a fait remarquer que l'« [o]n s'attendait à ce que les nouveaux pouvoirs d'enquête entraînent de nombreuses contestations fondées sur la Charte, mais cela ne s'est pas encore avéré » (JUS, 2020). Au-delà des mandats et ordonnances de communication, les forces de l'ordre disposent de peu d'indications sur les outils qu'ils peuvent utiliser pour accéder aux données dans le cadre d'une enquête, ce qui ouvre la porte à des atteintes à protection des renseignements personnels si les outils sont employés de manière inappropriée (section 6.3.5).

Les forces de l'ordre ont besoin de mandats pour accéder aux renseignements de base sur les abonnés (RBA)

L'accès aux RBA — qui peuvent comprendre le nom, l'adresse IP, l'adresse physique, le numéro de téléphone et l'adresse électronique d'un abonné — par les forces de l'ordre continue de faire l'objet de débats au Canada. Dans l'affaire *R. c. Spencer,* la Cour suprême du Canada a conclu que ces renseignements ne peuvent être obtenus sans autorisation judiciaire préalable en l'absence de « circonstances contraignantes » (CSC, 2014b), et que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ne confère pas aux forces de

l'ordre l'autorité légitime d'exiger de tels renseignements de leurs dépositaires. En bref, les forces de l'ordre ne peuvent pas demander des RBA à un fournisseur de services, car l'obtention de renseignements permettant aux autorités d'établir un lien entre l'identité d'une personne et ses activités en ligne constitue une perquisition protégée par la Constitution. Avant cet arrêt de 2014, la police obtenait régulièrement ce genre de renseignements directement des fournisseurs de services (JUS, 2020).

Comme il n'existe pas de loi spécifiquement pensée pour permettre l'accès aux RBA, la pratique actuelle est souvent de recourir à une ordonnance de communication générale, qui est applicable à tout type de renseignement (NLCA, 2019; JUS, 2020). À noter que dans l'affaire *R. c. Bykovets*, la Cour d'appel de l'Alberta a statué que la police pouvait légalement obtenir une adresse IP sans autorisation judiciaire, car « une adresse IP ne révèle pas à la police où elle se trouve ni, d'ailleurs, qui l'utilise. Il n'existe pas non plus de ressource accessible au public à partir de laquelle la police pourrait obtenir ces données ou d'autres données sur les abonnés » [traduction libre] (ABCA, 2022)[21]. Dans cette affaire, la police a ensuite utilisé une ordonnance de communication pour obtenir le nom et l'adresse de l'abonné associés à l'adresse IP.

Depuis l'arrêt *R. c. Spencer,* certains efforts ont été déployés pour créer des mécanismes qui permettraient aux forces de l'ordre d'accéder aux RBA sans mandat, souvent en invoquant le besoin perçu d'identificateurs de référence ou une enquête sur du matériel d'abus pédosexuels (MAP) (Parsons, 2022). Cependant, le débat se déplace souvent vers l'autorisation de l'accès aux RBA pour toutes les enquêtes ou même pour les actes non criminels (Parsons, 2022).

Les mécanismes actuels d'accès aux données hébergées hors Canada sont considérés par les services de police comme lents et lourds

Même lorsqu'une ordonnance judiciaire a été obtenue, il peut être difficile d'accéder à des données pouvant constituer des preuves criminelles (p. ex. noms d'utilisateur, adresses IP) auprès des fournisseurs de services (Carter et Daskal, 2018). Par exemple, il n'est pas toujours facile d'identifier les fournisseurs de services qui ont accès aux preuves numériques pertinentes recherchées, ou qui les possèdent carrément (Carter et Daskal, 2018). Le processus d'accès à l'information est parfois lourd, même lorsque le dépositaire de données a été déterminé. Des études s'appuyant sur des entrevues révèlent la frustration des enquêteurs canadiens sur les crimes sexuels, qui ont constaté que les procédures légales qui « étaient autrefois très courtes pour accéder au domicile d'un individu prennent

21 Cette décision a été portée en appel devant la Cour suprême du Canada (CSC, 2022).

maintenant plusieurs jours [...] pour obtenir quelque chose comme une adresse IP » [traduction libre] (Dodge *et al.*, 2019). Les participants à l'étude ont également décrit les processus d'obtention de mandats internationaux comme longs et laborieux lorsqu'ils cherchent à accéder à des renseignements auprès d'entreprises situées à l'extérieur du Canada, comme Meta.

Si les données sont hébergées à l'extérieur du Canada, la *Loi sur l'entraide juridique en matière criminelle* confère au ministère de la Justice le pouvoir légal de demander des ordonnances judiciaires dans les pays qui ont conclu un accord d'entraide juridique (AEJ) avec le Canada (GC, 2019d; JUS, 2020). Au cours de l'exercice 2017–2018, le ministère a déposé 114 demandes en vertu d'un AEJ dans le but d'obtenir des preuves numériques, contre 128 l'année précédente. Ce chiffre est nettement inférieur au nombre de demandes qu'il a reçues pour des preuves numériques hébergées au Canada (448 en 2017–2018) (JUS, 2020). Une évaluation de l'Initiative sur les pouvoirs d'enquête au 21e siècle (PE21S) a révélé que « [p]lusieurs représentants des organismes canadiens d'application de la loi ont déclaré qu'ils éviteront le long processus d'EJ, si possible » (JUS, 2020). Parsons (2016) note toutefois que, « si la lenteur de l'accès à l'information par le biais des [traités d'entraide judiciaire (TAJ)] est un problème pour les autorités canadiennes, ce problème ne peut pas être réglé par une nouvelle loi canadienne. La correction du processus de recours aux TAJ nécessitera plutôt des ressources supplémentaires dans le pays destinataire du mandat pour accélérer l'examen de ce mandat » [traduction libre].

Les difficultés liées aux TAJ auxquelles sont confrontés les organismes canadiens d'application de la loi pourraient s'atténuer dans les prochaines années. En effet, le Canada et les États-Unis ont entamé des négociations dans le cadre de la CLOUD Act américaine (section 5.2.5) afin de permettre aux autorités canadiennes d'adresser des ordonnances judiciaires directement aux fournisseurs américains pour obtenir les renseignements qu'ils détiennent sur des résidents canadiens soupçonnés d'un crime (DOJ, 2022b). Si ces négociations aboutissent et que des processus appropriés sont mis en œuvre, le temps et les efforts nécessaires pour obtenir des renseignements auprès d'entreprises américaines seront considérablement réduits, mais cela ne résoudra pas les problèmes associés aux TAJ lorsque les renseignements sont détenus en dehors du Canada et des États-Unis.

6.3.2 Chiffrement

Les forces de l'ordre considèrent le chiffrement comme un obstacle aux enquêtes sur les activités criminelles

Le chiffrement est « le processus d'encodage des informations afin qu'elles ne puissent être comprises que par le destinataire prévu » [traduction libre] (Masoodi

et Rand, 2021). Il est essentiel à la sécurité nationale, à la protection des droits de la personne et à la sécurité publique (Gill *et al.*, 2018). Le chiffrement est utilisé comme méthode sécurisée d'envoi et de stockage de différents types de données, ce qui garantit leur « confidentialité, leur intégrité et leur authenticité » [traduction libre] (Masoodi et Rand, 2021) et protège les internautes des menaces criminelles. Il peut être appliqué aux données stockées dans un appareil ou un système particulier (c.-à-d. les données au repos) ou aux données transmises entre des applications ou par Internet (c.-à-d. les données en transit), qui sont souvent plus difficiles à déchiffrer (Parsons, 2019). De nombreuses applications de messagerie, telles que WhatsApp et Signal, recourent de plus en plus au chiffrement de bout en bout, grâce auquel « seuls l'expéditeur et le destinataire prévu peuvent voir le contenu du message en clair » [traduction libre] (Masoodi et Rand, 2021). Les applications de chiffrement jouent un rôle important dans la protection des données personnelles, de la vie privée (chapitre 2), de la propriété intellectuelle et de la cybersécurité (ACCP, 2016; SP, 2020). Elles « permettent également l'exercice des droits et libertés fondamentaux, notamment la liberté de pensée, de croyance, d'opinion, d'expression et d'association » [traduction libre] (Parsons, 2019).

Les appareils et les applications intègrent couramment le chiffrement dans leur fonctionnement normal. Si cette intégration peut protéger les individus, elle peut également restreindre les renseignements auxquels les forces de l'ordre peuvent accéder, même après avoir obtenu une autorisation judiciaire afin de récolter des preuves numériques. Pour les forces de l'ordre, le chiffrement est un obstacle aux enquêtes sur les cybercrimes et au recueil de preuves numériques; l'Association canadienne des chefs de police (ACCP) a déjà affirmé que le chiffrement était un défi pour les enquêtes, même lorsque des autorisations judiciaires légales sont obtenues (ACCP, 2016). Les difficultés posées par le chiffrement ont notamment été relevées dans le cadre d'enquêtes sur l'exploitation et les abus sexuels d'enfants en ligne, la cyberfraude, le crime organisé et l'extrémisme (ACCP, 2016; SP, 2017b). Reprenant ce point de vue, le gouvernement du Canada a publié une déclaration commune avec le Groupe des cinq soulignant les écueils que constitue le chiffrement (section 5.3).

Dans l'évaluation de l'Initiative PE21S, un procureur fédéral a fait remarquer que « le nombre d'écoutes électroniques autorisées a diminué de façon spectaculaire au cours des dernières années en raison du chiffrement » et a constaté que cela avait conduit la police « à recourir à d'autres moyens de découvrir de l'information » (p. ex. des agents d'infiltration) (JUS, 2020); aucune de ces informations, cependant, n'a été énoncée dans un rapport du gouvernement provincial ou fédéral sur l'utilisation des écoutes au Canada (Parsons et Molnar, 2018). Parmi les autres raisons expliquant le déclin des écoutes téléphoniques, on

peut citer l'utilisation d'outils numériques (p. ex. le piratage, les outils d'enquête intégrés ou ODIT). Il convient de noter que les ODIT[22] sont utilisés par les forces de l'ordre canadiennes, mais qu'ils ne sont pas inclus dans les rapports d'écoute électronique, malgré le fait que des ordonnances d'écoute électronique soient utilisées pour les déployer (ETHI, 2022 ; Forrest, 2022; GRC, 2022a).

Le Web clandestin pose des problèmes uniques aux forces de l'ordre

L'utilisation croissante de la technologie de chiffrement dans les systèmes et produits numériques a également mené à la création et à la propagation de marchés en ligne illicites, de réseaux en ligne anonymes et d'infrastructures de communication et de vente fonctionnant sur le Web clandestin (Lukings et Lashkari, 2022b) (section 4.2). L'environnement anonymisé rend difficile l'établissement d'un lien entre les activités criminelles sur le Web clandestin et des groupes ou des individus particuliers, car les forces de l'ordre ne peuvent souvent pas cerner ou retracer les preuves numériques dans cet espace. Bien que les forces de l'ordre canadiennes tentent de surveiller le contenu et les activités sur le Web clandestin, il n'existe actuellement aucun logiciel capable de « détecter et surveiller adéquatement les accès, les communications et les activités illégales, ainsi que le contenu chiffré transmis sur le Web clandestin » [traduction libre] (Lukings et Lashkari, 2022b).

En revanche, il existe des outils surveillant le Web clandestin à la recherche de types précis de contenu illégal. Par exemple, Projet Arachnid (encadré 6.1) balaye les forums du Web clandestin, et des avis de retrait peuvent être produits dans les cas où les publications sont liées à des fichiers hébergés sur le Web ouvert (CCPE, 2021). On dispose d'une multitude d'outils de moissonnage automatique qui surveillent le Web clandestin à la recherche de données (AlKhatib et Basheer, 2019); ces outils sont utilisés par les particuliers pour déterminer si leurs données personnelles ont été compromises, mais aussi par les entreprises privées pour vérifier si la confidentialité de leurs données (qui peuvent inclure des renseignements sur leurs clients ou leurs utilisateurs) a été violée.

Les difficultés à accéder aux données chiffrées ne sont pas uniquement d'ordre technique

Si le chiffrement est considéré par les forces de l'ordre comme un obstacle aux enquêtes, la mesure dans laquelle il perturbe ou retarde ces enquêtes n'est pas tout à fait claire. Les rapports fédéraux et provinciaux sur la surveillance électronique au Canada ne mentionnent pas les difficultés que le chiffrement pose

22 Les ODIT sont des programmes informatiques installés sur un appareil comme un smartphone, à l'insu de son propriétaire, afin de permettre aux forces de l'ordre de recueillir des preuves numériques (GRC, 2022b).

à l'interception des communications (Parsons et Molnar, 2018). Si le chiffrement ralentit certaines enquêtes criminelles, il ne les empêche pas nécessairement, et les forces de l'ordre disposent d'autres moyens ne nécessitant pas le déchiffrement pour accéder aux preuves (p. ex. obtenir des ordonnances de communication pour accéder aux sauvegardes dans le nuage) (Parsons, 2019; West et Forcese, 2020; Masoodi et Rand, 2021).

Dans certains cas, la GRC a cité le chiffrement comme un problème, mais, après analyse, les problèmes relevés ne semblaient pas insurmontables (Parsons, 2016); les principaux défis répertoriés par la GRC étaient liés à des facteurs dépassant le chiffrement lui-même. Il s'agissait notamment des retards dans le recueil des preuves, du dysfonctionnement ou de la mauvaise utilisation de l'équipement, de l'incapacité à utiliser d'autres outils de recueil des données accessibles et du manque de coopération des fournisseurs de services Internet et de télécommunications (ACCP, 2016; Parsons, 2016; Powell et Henry, 2018). En outre, les forces de l'ordre font remarquer qu'elles ne disposent pas des outils technologiques et de l'expertise nécessaires pour combattre le chiffrement (Boutilier, 2016; Masoodi et Rand, 2021), ce qui indique qu'on est peut-être devant un problème de ressources et de personnel autant qu'un problème purement technique.

Les points d'accès aux dispositifs chiffrés par porte dérobée ou porte d'entrée permettent aux forces de l'ordre d'y accéder, mais introduisent des vulnérabilités

Il serait possible de surmonter les obstacles techniques posés par le chiffrement au moyen de particularités de conception. Comme pour les écoutes téléphoniques, les appareils pourraient être conçus pour permettre aux forces de l'ordre d'accéder aux données par une porte dérobée, dans des circonstances limitées. Cette méthode a fait ses preuves. De nombreux fournisseurs de messagerie chiffrent les messages, mais conservent une clé des communications hébergées sur leurs serveurs (Finklea, 2021). En 2010, la GRC a obtenu une clé de déchiffrement pour les appareils BlackBerry grand public. Grâce à cette clé, les enquêteurs ont pu déchiffrer plus d'un million de communications entre les membres d'une organisation mafieuse (Ling et Pearson, 2016; Pearson et Ling, 2016). On craint toutefois qu'un point d'entrée par porte dérobée soit inévitablement exploité par des acteurs malveillants (Dheri et Cobey, 2019; Dupont, 2021). Ce genre de point d'accès réduit l'intégrité structurelle des systèmes numériques et introduit des vulnérabilités. Comme l'expliquent Dheri et Cobey (2019), « on ne peut pas créer des portes dérobées pour rendre vulnérables les communications criminelles sans, en même temps, rendre les communications gouvernementales et individuelles susceptibles d'être piratées par des criminels, des terroristes ou des étrangers » [traduction libre].

Des responsables de l'application de la loi affirment que le terme d'*accès par porte dérobée* a une connotation de secret et lui préfèrent le terme d'*accès par porte d'entrée*, qui permet de « comprendre clairement quand on accède à un dispositif » [traduction libre] (Finklea, 2021). Cet accès serait fourni par le détenteur de la clé (ou par les détenteurs de la clé dans le cas d'une clé de chiffrement multipartite) si les enquêteurs ont démontré qu'ils ont une base légale pour accéder aux documents (Nakashima et Gellman, 2015; Finklea, 2021). Cette méthode se heurte au même problème fondamental, à savoir l'intégration de vulnérabilités potentielles dans le système.

En l'absence de points d'entrée par porte dérobée, les forces de l'ordre canadiennes ont besoin de directives claires sur ce qu'elles peuvent faire pour contourner le chiffrement. Dheri et Cobey (2019) suggèrent que les forces de l'ordre conçoivent leurs propres outils pour pirater les logiciels, afin de régler ce problème, mais le moment où ces outils peuvent être appliqués reste ambigu. Certains juristes se sont interrogés sur la manière dont les forces de l'ordre pourraient légalement employer ce type de piratage. Bellovin et al. (2014) soutiennent que le piratage légal devrait exploiter les vulnérabilités existantes, et que ces vulnérabilités soient signalées dès leur découverte ou leur achat au vendeur, ce qui pourrait conduire à un renforcement de la sécurité globale. Parsons (2014), constatant une dichotomie dans le contexte des « logiciels malveillants conçus pour ou achetés par les organismes gouvernementaux[23] » [traduction libre], explique :

> *S'il se lance dans le piratage informatique, le gouvernement du Canada se contredit lui-même : d'une part, il a mis en place des organismes pour mieux sécuriser l'infrastructure numérique gouvernementale et commerciale essentielle et d'autre part, les logiciels gouvernementaux seraient fondamentalement plus utiles s'il n'existait aucun moyen pour les personnes ciblées de détecter ou de bloquer leur présence ou leurs activités.*

En outre, des entreprises qui fabriquent des outils de piratage légaux ont subi des violations de la confidentialité des données, qui ont révélé que ces outils sont vendus à des gouvernements qui commettent de graves violations des droits de la personne. En 2015, par exemple, Hacking Team, un concepteur d'outils technologiques destinés à des gouvernements et des forces de l'ordre et dont le siège est à Milan, a signalé la fuite de près de 400 Go de ses données internes, notamment des fichiers clients et des données financières, à cause de pirates informatiques (Singh, 2015). Ces données ont révélé que Hacking Team avait vendu ses logiciels à plusieurs pays qui violent les droits de la personne, notamment l'Éthiopie, le Kazakhstan, la République du Soudan et l'Arabie saoudite. Ces outils de piratage peuvent être utilisés pour des activités qui sont techniquement

23 Le *govware*, en anglais [NdT].

considérées comme légales dans ces pays, mais qui seraient considérées comme illégales du point de vue des lois canadiennes ou internationales. En outre, le Centre canadien pour la cybersécurité (2022a) note qu'« [i]l est fort probable que des gouvernements étrangers ont utilisé ces outils commerciaux contre des Canadiens et des groupes d'intérêt au Canada ».

La manière dont ces outils sont utilisés par les gouvernements des pays démocratiques suscite également des inquiétudes. Une enquête menée par Citizen Lab, en collaboration avec des groupes de la société civile, a révélé qu'au moins 65 personnes en Catalogne ont été ciblées ou infectées par des logiciels espions de NSO Group (Pegasus) ou Candiru (Scott-Railton *et al.*, 2022). Il s'agit dans les deux cas de sociétés de surveillance mercenaires qui vendent leurs logiciels espions à des clients gouvernementaux. Au nombre des personnes visées figurent des militants, des universitaires, des élus et des membres du gouvernement catalan, ainsi que des personnes résidant dans d'autres pays de l'UE et en Suisse. L'enquête n'a pas attribué de manière concluante les attaques à « un gouvernement particulier », mais a noté que « de nombreuses preuves circonstancielles désignent le gouvernement espagnol » [traduction libre] (Scott-Railton *et al.*, 2022). Elle a également constaté que le logiciel espion était actif lorsque les responsables catalans et le gouvernement espagnol étaient en négociations sur l'autonomie de la Catalogne.

6.3.3 Traitement et partage des preuves numériques

L'automatisation peut améliorer l'efficacité de la criminalistique numérique

Comme nous l'indiquons à la section 6.2.1, les contraintes de personnel créent un goulot d'étranglement dans le traitement des preuves numériques. Ces contraintes sont aggravées par des processus inefficaces, qui font que les examinateurs judiciaires passent leur temps à effectuer des tâches répétitives et banales. Lorsque les appareils numériques sont examinés « individuellement », un seul examinateur judiciaire numérique doit faire passer chaque appareil par toutes les étapes de l'enquête sur un même poste de travail (Saliba, 2021). Comme l'explique Jad Saliba (2021), fondateur et directeur technique de Magnet Forensics, « de nombreuses tâches requises sont élémentaires et ne demandent rien de plus que brancher un appareil ou cliquer sur des invites » [traduction libre]. Il est donc possible de recourir à l'automatisation pour effectuer les tâches banales et répétitives, afin que les experts juridiques puissent se consacrer à l'analyse des données et à la fourniture des données extraites aux enquêteurs.

Le recours à l'automatisation peut également ouvrir la voie au traitement simultané des données de plusieurs appareils à la fois et contribuer à la

standardisation du flux de travail. Les corps policiers ont d'ailleurs reconnu la nécessité d'une automatisation croissante. Par exemple, le responsable de la technologie à la Fédération policière d'Angleterre et du Pays de Galles a noté « la nécessité pour les forces d'investir dans la technologie qui peut accélérer ce processus en extrayant et en triant les données des appareils numériques automatiquement » [traduction libre] (ITV News, 2020). En fin de compte, l'automatisation pourrait accroître la productivité, réduire le temps requis pour traiter un appareil numérique et assurer la cohérence. Le comité d'experts note que tout système de criminalistique numérique, ainsi que ses processus automatisés, doit être accessible à l'évaluation par les avocats de la défense pour s'assurer que les défendeurs dans les affaires criminelles ont toute possibilité de monter leur défense.

Les outils rendant les preuves numériques plus accessibles aux forces de l'ordre pourraient accélérer les enquêtes

Il y a des délais concernant les preuves numériques, même après l'extraction des données d'un appareil. Actuellement, il est difficile pour les enquêteurs non techniciens d'accéder aux données extraites de dispositifs numériques. C'est pourquoi, dans de nombreux cas, les agents qui connaissent le mieux une enquête ne reçoivent que des rapports statiques (une fois que les examinateurs judiciaires ont pu les préparer), à moins de recourir à un processus chronophage pour accéder aux données (p. ex. aller voir l'examinateur judiciaire, apprendre à se servir d'un logiciel complexe utilisé par les examinateurs) ou d'obtenir les données par des méthodes qui introduisent une vulnérabilité (p. ex. partage de clés USB). Ce problème pourrait être atténué grâce à un système simplifié d'examen des preuves, qui permettrait aux agents de se connecter en toute sécurité et d'analyser eux-mêmes ces preuves. Ce système devrait être accompagné de processus permettant une surveillance indépendante, garantissant la préservation de la chaîne de conservation des preuves et assurant que les agents ne peuvent pas modifier accidentellement ou intentionnellement les renseignements obtenus par l'informatique judiciaire. Des systèmes de preuve accessibles et efficaces contribueraient à éliminer certains des goulots d'étranglement liés au transfert des données des affaires dans le système judiciaire.

6.3.4 Détection et rapports numériques

On peut recourir à des outils numériques pour détecter le MAP en ligne

Il est possible d'utiliser des outils de détection multimodale automatisés pour détecter le MAP, lesquels surveillent les images et les noms de fichiers en ligne et

évaluent plusieurs variables. Par exemple, on peut appliquer un algorithme de hachage perceptuel de mise en correspondance d'images au MAP, comme c'est le cas avec PhotoDNA de Microsoft, qui est utilisé pour comparer les images accessibles au public avec celles conservées dans la base de données du National Center for Missing and Exploited Children (NCMEC) (Westlake *et al.*, 2012; Edwards *et al.*, 2021). Cette technique améliore l'efficacité dans la mesure où elle est plus rapide que le recours à des agents pour analyser visuellement les images (Edwards *et al.*, 2021). Certains programmes automatisés se déplacent entre de multiples sites Web en suivant des liens connexes une fois activés sur un site de MAP connu (Edwards *et al.*, 2021). Ce processus permet de déterminer le volume de MAP tout en aidant les forces de l'ordre à suivre le chemin de la diffusion, l'objectif final étant de démanteler un site central et d'empêcher tout accès et toute distribution futurs parmi les utilisateurs (Westlake *et al.*, 2012; Edwards *et al.*, 2021). Un exemple populaire d'un tel outil est Projet Arachnid, qui a eu un effet considérable sur la capacité des enquêteurs à détecter et à traiter les images de MAP (encadré 6.1). Il est important de noter que les stratégies de cyberdétection automatisée peuvent être particulièrement utiles pour la santé des enquêteurs mêmes, car le visionnement répété d'images préjudiciables au travail leur fait courir un risque accru de stress traumatique secondaire (Burns *et al.*, 2008).

Les robots Web présentent certaines limites, notamment à cause du temps et des ressources nécessaires pour former les agents à leur utilisation et la sélection des mots-clés les plus efficaces et qui aboutissent aux meilleurs résultats (Edwards *et al.*, 2021). De plus, les robots Web nécessitent des protections efficaces et des mécanismes de surveillance continue pour s'assurer qu'ils ne servent pas à accéder à des données qui seront ensuite traitées à des fins autres que la recherche de MAP.

Encadré 6.1 Projet Arachnid

Lancé en 2017 par le Centre canadien de protection de l'enfance (CCPE), Projet Arachnid est un outil automatisé qui balaye le Web ouvert et le Web clandestin à la recherche de MAP ou d'autres documents préjudiciables et répréhensibles concernant les enfants (CCPE, 2021). Le système peut détecter des dizaines de milliers d'images par seconde. Une fois qu'une image illégale a été détectée, il envoie des avis de retrait aux sites hébergeant le contenu (CCPE, 2021). Le CCPE travaille en collaboration avec des partenaires mondiaux, y compris des ONG internationales et des lignes de signalement de MAP. Cette collaboration permet de réduire les doublons et d'augmenter le nombre d'avis de retrait unique pour du MAP (CCPE, 2017).

Projet Arachnid est un modèle centré sur la victime, en ce sens qu'il est destiné à faciliter la détection et le retrait précoces. Il réduit ainsi les risques que les victimes et les survivants tombent sur du matériel ou que ce matériel soit distribué ou reproduit sur des sites Web (CCPE, 2017). En plus de traiter les images en temps réel, Projet Arachnid collecte des données qui peuvent être utilisées par la communauté internationale pour évaluer l'ampleur de l'exploitation en ligne des enfants, ainsi que les moyens possibles de remédier aux préjudices (CCPE, 2017). En 2021, Projet Arachnid a détecté et vérifié 5,4 millions d'images et envoyé des avis de retrait à 760 fournisseurs de services dans le monde, au rythme d'environ 3500 avis quotidiens (CCPE, 2021).

Le signalement en ligne est utilisé au Canada pour détecter le MAP

Les fournisseurs de services Internet au Canada sont tenus de signaler les sites qui hébergent du MAP à Cyberaide.ca (GC, 2011b; Cyberaide.ca, s.d.), et les particuliers sont également encouragés à signaler des actes potentiellement préjudiciables ou illégaux sur la ligne de dénonciation. Cyberaide.ca se veut un moyen simple et anonyme de signaler un comportement suspect ou inquiétant. Il reçoit les signalements de MAP, de leurre d'enfant, de diffusion non consensuelle d'images intimes, de mise à la disposition d'un enfant de matériel sexuellement explicite, d'entente avec une autre personne pour perpétrer une infraction sexuelle contre un enfant, d'exploitation sexuelle d'enfants à des fins commerciales, de traite des enfants et de tourisme sexuel impliquant des enfants (Cyberaide.ca, 2022b). Les signalements peuvent être effectués par n'importe qui, mais le comportement préjudiciable doit viser des enfants ou des adolescents de moins de 18 ans. La *Loi sur les services à l'enfant et à la famille* du Manitoba rend obligatoire le signalement

de la pornographie juvénile au CCPE, qui exploite Cyberaide.ca (Gouv. du Man., 2014, 2022). La Nouvelle-Écosse rend également obligatoire le signalement du MAP, mais dans cette province, l'entité responsable du signalement est tout organisme d'application de la loi (Gouv. de la N.-É., 2008).

Cyberaide.ca a été lancé sous forme de projet pilote en 2002 (CCPE, 2017) et a été officiellement adopté en 2004 dans le cadre de la Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet. À la réception d'un signalement, Cyberaide.ca évalue et trie les renseignements pour aider les forces de l'ordre à déterminer la criminalité et la compétence (CCPE, 2017). Cet organisme est exploité par le CCPE et soutenu par l'ACCP, la GRC et le Service canadien de renseignements criminels; en tant qu'élément du CCPE, il a signé des protocoles avec 28 services de police du Canada dans le but de leur fournir des ressources destinées au public (Cyberaide.ca, 2022c). Les objectifs et la stratégie de la ligne de signalement ont évolué depuis sa création, en grande partie grâce aux nouveaux services offerts par Projet Arachnid. En 2021, le service de signalement public de Cyberaide.ca (Projet Arachnid exclu) a traité plus de 360 000 signalements. Parmi ceux-ci, plus de 23 300 ont été transmis aux forces de l'ordre, plus de 1 000 aux organismes de protection de l'enfance et plus de 127 300 ont été « retransmis à l'international » (Cyberaide.ca, 2022d).

Cyberaide.ca, ainsi que les sites partenaires du CCPE, offre également des ressources pour aider les victimes à faire retirer d'Internet les photos ou les vidéos les représentant. Ces ressources comprennent des modèles de lettre et les coordonnées des platesformes de médias sociaux populaires (AidezMoiSVP.ca, 2022). Par exemple, le site AidezMoiSVP.ca offre des conseils sur la façon de faire retirer du contenu sensible des services en ligne, de contacter leurs auteurs, de contacter les forces de l'ordre (p. ex. quand et comment), d'obtenir des conseils juridiques et d'aider les victimes et les survivants à trouver le soutien dont ils ont besoin. Cyberaide.ca ne fournit pas seulement des services aux victimes et aux survivants âgés de moins de 18 ans, une grande partie des conseils et des ressources que ce site et AidezMoiSVP.ca procurent peuvent être utiles à toute personne préoccupée par la diffusion non consensuelle d'images intimes. Il ne semble pas exister de service officiel de signalement comparable à Cyberaide.ca pour les adultes au Canada.

Le signalement en ligne est utilisé dans d'autres pays pour aider les adultes victimes et survivants d'abus sur Internet à partir d'images

Des portails semblables à Cyberaide.ca existent dans le monde entier et sont souvent connectés par l'intermédiaire d'INHOPE, une organisation internationale qui regroupe environ 50 lignes d'assistance ou de signalement réparties dans

40 pays et dédiées au signalement et à l'élimination du MAP (INHOPE, 2020). Il fournit du matériel éducatif et des outils avancés pour aider les lignes d'assistance téléphonique des pays membres à partager efficacement les cas signalés, à faire remonter les nouveaux cas et à réduire le nombre de dédoublements d'enquêtes (INHOPE, 2020). Dans certains cas, les lignes d'assistance téléphonique associées sont équipées pour traiter tous les niveaux d'images intimes préjudiciables, tandis que d'autres se concentrent exclusivement sur le MAP (INHOPE, 2020).

Le gouvernement australien propose un organisme comparable à Cybertip.ca dans son portail de sécurité en ligne, esafety.gov.au. Ce site Web est destiné à fournir des renseignements, des ressources et des outils de signalement afin de mieux protéger la population australienne sur Internet (Yar et Drew, 2019; Commissaire à la sécurité électronique, 2021b). Alors que 73 % des cas d'abus à partir d'images signalés entre 2020 et 2021 visaient des adultes, ce portail a fait remarquer qu'il ne disposait pas de pouvoirs officiels pour enquêter sur les cas de cyberabus d'adultes (Commissaire à la sécurité électronique, 2021b). Cependant, en janvier 2022, de nouvelles lois sur la sécurité en ligne sont entrées en vigueur et ont élargi sa capacité à aider les adultes victimes de préjudices en ligne (Commissaire à la sécurité électronique, 2022a).

Pour déclencher une enquête du commissariat à la sécurité électronique, il faut que le signalement satisfasse certains critères de contenu (p. ex. qu'il comprenne des images intimes réelles ou fausses) et qu'il ait été fait par la personne représentée sur l'image intime (ou par son parent ou tuteur dans le cas d'un mineur) ou par une personne autorisée à faire un signalement en son nom (Yar et Drew, 2019; Commissaire à la sécurité électronique, 2022b). Si ces critères sont remplis, le Commissaire a le pouvoir de lancer le retrait des images intimes, de fixer des amendes et des sanctions ou de prendre d'autres mesures réglementaires contre le responsable. En 2021, le commissariat à la sécurité électronique a pu faire retirer sur demande 90 % du matériel répréhensible à base d'images (Commissaire à la sécurité électronique, 2021b). Malgré les succès de l'approche australienne, les grandes entreprises technologiques américaines telles que Meta, Google et Apple (représentées par le groupe industriel DIGI) estiment que les lois australiennes sur la sécurité en ligne sont incohérentes, déroutantes et difficiles à respecter; ces entreprises ont donc demandé que toutes les nouvelles lois soient simplifiées en un seul texte législatif (Brookes, 2022).

6.3.5 Intelligence artificielle (IA)

Les applications qui utilisent l'IA présentent des avantages potentiels pour les forces de l'ordre, mais elles comportent également des dimensions uniques en matière d'éthique et de vie privée

Bien que la définition de l'*IA* soit évolutive, le terme est utilisé dans ce rapport pour décrire les utilisations assistées par la machine, y compris celles basées sur l'apprentissage automatique, l'apprentissage profond et l'apprentissage par renforcement (CAC, 2022). Les progrès réalisés en matière de matériel et de logiciels, la disponibilité d'énormes quantités de données et l'intérêt croissant de l'industrie pour l'IA ont conduit à la conception d'applications dans de nombreux domaines, notamment dans la prise de décision et l'application de la loi. À l'avenir, il est probable que « peu de champs seront laissés intacts par l'IA » (CAC, 2022).

Alors que l'IA peut être fréquemment utilisée pour l'application de la loi — par exemple, pour aider à localiser des suspects ou des victimes ou pour détecter des délits tels que la fraude —, leur emploi suscite de nombreuses préoccupations, et l'on manque de guide pour savoir quand un outil particulier est approprié. En premier lieu, on craint que des renseignements personnels puissent être divulgués durant le recueil de données provenant de sources sur lesquelles un outil d'IA est entraîné ou appliqué; on a constaté que de nombreux grands ensembles de données et les algorithmes d'IA qui leur sont associés reposent sur la collecte ou l'analyse non consensuelle de données (Leslie, 2020). Les applications d'IA ont également le potentiel de perpétuer, voire d'amplifier, la discrimination et les préjugés inhérents aux ensembles de données utilisés pour les entraîner (Barocas et Selbst, 2016). Il s'agit d'un risque considérable dans un contexte d'application de la loi en raison de l'historique de racisme systémique des systèmes de maintien de l'ordre au Canada (SECU, 2021). Il existe également des risques que les applications d'IA souffrent du « problème de la boîte noire », c'est-à-dire qu'il est difficile, voire impossible dans certains cas, de demander aux algorithmes d'apprentissage automatique et d'IA comment ils fonctionnent (section 2.1.2); cela pose des problèmes fondamentaux pour l'administration de la justice lorsque les boîtes noires empêchent un défendeur de mettre sur pied une défense complète, ou lorsque des personnes ont des interactions négatives avec les forces de l'ordre à cause de biais de *mathwashing*[24] des algorithmes (Robertson *et al.*, 2020). En raison de ces risques, il est important d'assurer la transparence, l'évaluation indépendante et le suivi des questions éthiques et des données d'entrée utilisées pour l'IA dans les forces de l'ordre (section 6.3.6). Comme un rapport du CAC (2022) le constate, « [c]ertains de ces risques sont dus aux écarts entre les principes de

24 Le fait de croire que les algorithmes sont neutres et objectifs [NdT].

développement responsable de l'IA et leur opérationnalisation, ainsi qu'à l'insuffisance globale de solides mesures réglementaires ».

Il est possible de tirer parti de l'IA et de l'analyse croisée des cas pour favoriser la détermination et le partage des données

Il est possible d'utiliser des applications d'IA pour accélérer l'analyse des preuves numériques *et al*léger le fardeau imposé aux agents et au personnel chargés de l'informatique judiciaire (Rigano, 2019). L'IA peut servir à déterminer les données pertinentes qui fournissent un point de départ aux enquêteurs. Ainsi, les techniques numériques, y compris les systèmes d'IA, peuvent découvrir des preuves utiles à une affaire plus rapidement qu'une méthode manuelle (Novak *et al.*, 2019; Shute *et al.*, 2021). Par exemple, une entreprise technologique a constaté que l'IA permettait de balayer les messages texte à la recherche de certaines phrases ou de certains sujets au lieu de lire entièrement chaque message et pouvait montrer comment certains artefacts sont reliés les uns aux autres (Police1 BrandFocus Staff, 2018).

Il est toutefois important de tester et de superviser ces outils de manière appropriée, car les analyses de certains outils d'enquête automatisés révèlent des biais, ce qui pourrait conduire à une intervention policière excessive dans certaines communautés à cause des interactions passées avec les forces de l'ordre (Koepke *et al.*, 2020).

L'IA pourrait être utilisée pour étayer l'analyse croisée des cas entre les forces de l'ordre, ce qui est particulièrement important pour les crimes cyberfacilités pour lesquels les preuves (ainsi que les auteurs et les victimes) peuvent relever de plusieurs compétences. Le comité d'experts constate que, en l'absence de protocoles d'entente et d'autorisation spécifique d'accès aux renseignements liés aux procédures criminelles, ces systèmes devraient être conçus pour interagir sans révéler les détails des affaires aux différents organismes.

Les forces de l'ordre ont utilisé la technologie de reconnaissance faciale pour faciliter des enquêtes

La technologie de reconnaissance faciale (TRF) informatisée est un type d'identification biométrique qui repose sur des images telles que les photos de passeport et les photos d'identité judiciaire (CPVC, 2011; Crumpler et Lewis, 2021). Le TRF prend une image du visage d'une personne et la traduit en données, qui peuvent être comparées quantitativement à d'autres données faciales (EFF, 2017; Crumpler et Lewis, 2021). De nombreux algorithmes de reconnaissance faciale reposent sur les mesures de la taille, de la forme et de l'emplacement relatif des traits du visage, qui sont ensuite comparées à d'autres de façon individuelle

(c.-à-d. comparaison de deux images pour déterminer si elles proviennent de la même personne) ou collective (c.-à-d. recherche d'une correspondance dans une base de données) (Crumpler et Lewis, 2021). L'accès à un calcul performant, aux techniques de traitement parallèle et aux platesformes dans le nuage a accéléré la recherche et permis de surmonter les difficultés d'identification et d'extrapolation des objets dues aux différences d'éclairage et d'angle de prise de vue et aux expressions faciales changeantes.

Actuellement, les données de TRF sont moins précises que les autres formes de données biométriques, mais le procédé ne requiert aucun contact (contrairement à la numérisation des empreintes digitales) et peut reposer sur une imagerie de moindre résolution ou de mauvaise qualité (par rapport à la numérisation de l'iris). Il en résulte que la TRF peut être utilisée pour identifier des individus dans les espaces publics et pour le marquage automatique d'images (Robertson, 2021), souvent à l'insu des personnes surveillées. Alors qu'on sait probablement quand ses empreintes digitales sont scannées, il n'en va pas de même pour la surveillance optique. À ce jour, les gouvernements et les forces de l'ordre ont utilisé la TRF pour tout un ensemble de raisons, notamment la vérification de l'identité aux frontières, la vérification de l'admissibilité aux services gouvernementaux et la génération de pistes pour aider à retrouver des personnes recherchées (p. ex. Braga, 2017; Robertson *et al.*, 2020; Rakheja, 2021).

L'utilisation de la TRF par les forces de l'ordre a entraîné des violations de la vie privée au Canada

À mesure que les algorithmes de reconnaissance faciale s'améliorent et que les bases de données s'étoffent, il devient possible d'identifier n'importe qui dans la rue et de voir son historique d'arrestations, sa présence sur les médias sociaux et une foule de détails personnels — en temps réel et à partir d'une simple photographie (Klosowski, 2020). Alors que les experts techniques s'efforcent d'améliorer la fonctionnalité des systèmes de TRF, certains experts juridiques et éthiques ont averti que, même dans sa forme actuelle, la TRF menace le droit du public à la vie privée à cause de son recours à la surveillance publique généralisée, d'une façon unique à des exécutions particulières d'algorithmes de reconnaissance faciale (EFF, 2017; Robertson *et al.*, 2020).

La TRF peut, dans certains cas, faire le lien entre les pratiques traditionnelles de recours à des photos d'identité judiciaire et le maintien de l'ordre algorithmique, les photos d'identité judiciaire disponibles étant souvent utilisées pour constituer une base de données d'images faciales à analyser (Robertson *et al.*, 2020; Hao, 2021). Selon la *Loi sur l'identification des criminels* du Canada, les photos d'identité judiciaire peuvent être recueillies sans consentement lorsqu'un individu a été accusé ou condamné ou est présumé avoir commis un acte criminel (GC, 1985).

Les personnes déclarées innocentes ou pour lesquelles les charges ont été abandonnées ont le droit de faire détruire ces données (dans certains cas, cela ne se fait que sur demande) (Robertson *et al.*, 2020). Ces photos ne sont toutefois pas les seuls éléments que les logiciels de reconnaissance faciale peuvent utiliser pour constituer des bases de données d'images. Clearview AI, par exemple, a récolté plus de 10 milliards d'images faciales « à partir de sources Web exclusivement publiques, y compris les médias d'information, les sites Web de photos d'identité judiciaire, les médias sociaux publics et de nombreuses autres sources ouvertes » [traduction libre] (Clearview AI, 2021). En juin 2021, le Commissariat à la protection de la vie privée (CPVP) a statué que l'emploi de Clearview AI par la GRC violait les lois canadiennes sur la protection des renseignements personnels, car l'entreprise a construit sa banque de données à partir d'images récupérées sur Internet sans consentement. Le CPVP a conclu qu'« il incombait à la GRC (Gendarmerie royale du Canada) de s'assurer que la base de données qu'elle utilisait était compilée légalement », tandis que la GRC a soutenu « que cela créerait une obligation déraisonnable et que la loi n'impose pas expressément l'obligation de confirmer le fondement juridique de la collecte de données personnelles par ses partenaires du secteur privé » (CPVP, 2021c).

En juillet 2020, Clearview AI a annoncé qu'elle abandonnait volontairement son offre de services de reconnaissance faciale au Canada face aux enquêtes sur la protection de la vie privée menées dans tout le pays (Daigle, 2020), déclarant qu'elle était « prête à envisager le maintien de cette situation pendant deux années, afin de permettre aux différents commissaires de fournir des lignes directrices détaillées et logiques sur la manière dont l'intelligence artificielle pourrait être traitée dans le droit canadien » (CPVC, 2021d). À la suite d'une enquête conjointe avec le CPVP, les autorités de protection de la vie privée de trois provinces (Colombie-Britannique, Alberta et Québec) ont conclu que Clearview AI avait enfreint la législation sur la protection des renseignements personnels (y compris la LPRPDE) et ont recommandé que l'entreprise cesse de recueillir et d'utiliser des images de personnes sans leur consentement et supprime toutes les images et matrices faciales biométriques recueillies sans consentement (CPVP, 2021d)[25].

Des décisions similaires ont été rendues ailleurs. Au Royaume-Uni, le commissariat à l'information a ordonné à Clearview AI de cesser de recueillir ou d'utiliser des données sur des résidents du Royaume-Uni et de supprimer les données existantes de son système, à la suite d'une enquête conjointe avec le commissariat à l'information australien (ICO, 2022). Cette enquête bilatérale a révélé que Clearview AI avait violé la vie privée de citoyens au RoyaumeUni et en Australie (OAIC, 2021; ICO, 2022). Ces cas démontrent la légalité et l'éthique

25 Clearview AI Inc. a indiqué qu'elle ferait appel de ces décisions (Hill, 2021; Lyons, 2021).

douteuses associées à la création des systèmes de reconnaissance faciale de Clearview AI, qui ont été utilisés par des corps policiers au Canada et dans des pays pairs.

Ces questions éthiques, ainsi que la confection technique des bases de données faciales, sont rendues encore plus compliquées par le problème de la boîte noire. Lorsqu'un système de TRF produit une correspondance, il est souvent difficile de savoir si les biais dans les données analysées, dans les données d'apprentissage (dans le cas de l'apprentissage automatique) ou dans le fonctionnement de l'algorithme ont été correctement pris en compte (Buolamwini et Gebru, 2018). La reconnaissance faciale s'avère particulièrement problématique lorsqu'il s'agit d'identifier les personnes à la peau foncée et elle identifie le genre sur la base de stéréotypes dépassés (Buolamwini et Gebru, 2018; Simonite, 2018; NSF, 2019). Ce problème mène à une identification erronée des suspects dans les analyses de type « un à plusieurs », à des résultats médiocres dans les comparaisons d'images de type « un à un » et à des erreurs dans la détermination du sexe des sujets (Schiebinger *et al.*, 2021). Par conséquent, les critiques de la TRF ont soulevé des craintes à propos de l'utilisation de cette technologie, car elle renforce les préjugés policiers (p. ex. contre les personnes racisées) plutôt que les réduire (Condie et Dayton, 2020; Tsui, 2020). Ces biais techniques, ainsi que des préoccupations d'ordre éthique, ont conduit certaines villes et certaines forces de l'ordre à décréter un moratoire sur l'utilisation de la TRF, et des universitaires et défenseurs des libertés civiles ont demandé que les corps policiers cessent d'y recourir.

6.3.6 Surveillance et orientation

Sous réserve d'une surveillance et d'une orientation appropriées, la TRF et d'autres procédés basés sur l'IA peuvent aider les forces de l'ordre

L'un des sous-produits de la controverse entourant l'utilisation de la TRF au Canada pourrait être une baisse de la volonté des forces de l'ordre d'investir dans les technologies numériques, même si ces technologies ne posent pas les mêmes problèmes de confidentialité ou d'éthique que la TRF. Les problèmes engendrés par l'utilisation de la TRF par les forces de l'ordre canadiennes ne sont pas surprenants, car de nombreux experts — y compris des universitaires, des groupes de défense et des membres de la société civile — ont défini comment la technologie pourrait mal identifier les personnes racisées et ont prédit qu'elle entraînerait des violations de la vie privée (Braga, 2017; NSF, 2019; Hill, 2020; Leslie, 2020; Robertson *et al.*, 2020).

Étant donné que ces problèmes étaient prévus, certains ont fait remarquer qu'avec la réglementation, la surveillance et la transparence appropriées, la TRF pourrait être un outil précieux pour les enquêtes criminelles (Robertson *et al.*, 2020; CPVC, 2021c). Comme l'a expliqué Daniel Therrien, ancien commissaire à la protection de la vie privée du Canada, la TRF « a le potentiel d'offrir de grands avantages à la société. Cependant, la technologie de reconnaissance faciale peut être une technologie de surveillance très envahissante comportant de nombreux risques » (CPVP, 2021c). Reconnaissant l'utilité de la TRF, le CPVP, de concert avec ses collègues provinciaux et territoriaux, a élaboré une ébauche de directives à l'intention des services de police afin de s'assurer que « l'utilisation de celle-ci soit conforme aux lois actuelles et limite les risques d'atteintes à la vie privée » (CPVP, 2021c).

L'orientation et la surveillance de l'utilisation des nouvelles technologies dans le domaine de l'application de la loi peuvent aider à déceler les problèmes potentiels concernant la vie privée ou l'éthique avant leur mise en œuvre

Les problèmes de protection de la vie privée, de société et de droit qui découlent de l'utilisation des technologies numériques dans le domaine de l'application de la loi ne sont pas propres au Canada. D'autres pays ont mis en place des mécanismes pour déceler les éventuels problèmes juridiques et éthiques avant que des technologies nouvelles ou avancées soient utilisées. Le comité consultatif sur les technologies émergentes de Nouvelle-Zélande, qui fournit à la police néo-zélandaise des conseils accessibles au public, en est un exemple (encadré 6.2).

Au Canada, la GRC a créé en mai 2021 le Programme national d'intégration des technologies « afin de centraliser et de rendre plus transparents les processus qui régissent la façon dont la GRC sélectionne, évalue, surveille et approuve l'utilisation des technologies nouvelles et émergentes et des outils d'enquête qui requièrent la collecte et l'utilisation de renseignements personnels » (GRC, 2021e). Le comité d'experts n'est pas parvenu à trouver d'autres détails sur le programme ni à savoir s'il avait atteint, en juin 2022, le statut opérationnel. En 2022, le Toronto Police Services Board (conseil des services policiers de Toronto) a introduit une politique régissant l'emploi de l'IA (TPSB, 2022), qui stipule que toute utilisation de la technologie, y compris l'IA, doit respecter huit principes directeurs : « légalité, équité, fiabilité, justifiabilité, responsabilité personnelle et organisationnelle, transparence, respect de la vie privée et communication satisfaisante » [traduction libre]. De plus, les procédures et les processus d'examen et d'évaluation des nouveaux outils d'IA seront élaborés en consultation avec le commissaire à l'information et à la protection de la vie privée de l'Ontario, le ministère du Procureur général de l'Ontario et la Direction générale de l'action

contre le racisme de la province, ainsi que des experts et intervenants externes. L'examen et l'évaluation des nouvelles technologies incluent l'établissement d'une catégorie de risque de préjudice. L'approbation de la commission est requise avant l'acquisition, l'utilisation et le déploiement de nouvelles technologies; celles qui sont considérées comme présentant un risque extrême[26] ne sont pas approuvées et celles qui sont considérées comme présentant un risque élevé ou modéré font l'objet d'une surveillance supplémentaire par la commission et d'un rapport du chef de police (TPSB, 2022).

Encadré 6.2 Comité consultatif sur les technologies émergentes de Nouvelle-Zélande

Le comité consultatif sur les technologies émergentes de Nouvelle-Zélande (Advisory Panel on Emergent Technologies in New Zealand) a été créé pour conseiller la police néo-zélandaise, à partir du constat que les agents et le personnel « rencontrent de plus en plus de technologies émergentes dans leur travail quotidien » [traduction libre], qui peuvent leur permettre de s'acquitter de leurs tâches plus efficacement, mais qui sont susceptibles d'avoir d'importantes implications en matière d'éthique, de protection de la vie privée ou autres qu'il convient de prendre en compte (Police néo-zélandaise, 2021). Comme l'explique la Police néo-zélandaise (2021), « l'adoption de technologies qui ne sont pas perçues comme étant suffisamment bien comprises, acceptées par le public ou réglementées de manière appropriée a le potentiel de saper la confiance de la population dans l'organisme qui les déploie, en particulier lorsque les éventuels impacts négatifs (tels que l'atteinte à la vie privée ou des effets inéquitables sur certains groupes) peuvent être perçus comme dépassant les avantages publics » [traduction libre].

Le comité consultatif indépendant a pour objectif de formuler des conseils sur les conséquences politiques et éthiques des technologies émergentes (ou d'une « nouvelle fonctionnalité importante à l'intérieur d'une technologie existante » [traduction libre]) pouvant être utilisées dans le cadre de l'application de la loi. Il examine également les

(Continue)

26 Parmi les exemples de facteurs pouvant conduire à une désignation de « risque extrême », citons les utilisations pour lesquelles il n'y a pas d'humain qualifié pour évaluer la recommandation d'un outil d'IA, les utilisations qui conduisent à une surveillance de masse et les utilisations qui « prédisent ou attribuent la probabilité » pour une personne ou un « groupe de commettre un délit ou de récidiver » [traduction libre] (TPSB, 2022).

(a continué)

algorithmes utilisés par la police (Police néo-zélandaise, 2021). Un processus officiel a été mis en place, par lequel le commissaire de police (ou son représentant) soumet des questions au comité consultatif et précise le délai dans lequel les réponses sont demandées, généralement de l'ordre de quatre à huit semaines (plus, dans certains cas). Les conseils sont transmis au commissaire par écrit, accompagnés — le cas échéant — d'une présentation à un groupe de policiers (Police néo-zélandaise, 2021). Ce processus est confidentiel, mais la Police néo-zélandaise a fait remarquer qu'elle « s'engage à rendre public l'avis du comité d'experts dans la mesure du possible — tout en admettant que cela n'est pas toujours possible, par exemple si la communication violerait des obligations commerciales » [traduction libre] (Police néo-zélandaise, 2022). Les avis sont censés découler d'un consensus, mais les opinions divergentes de la majorité peuvent être enregistrées lorsque le consensus est impossible (Police néo-zélandaise, 2021).

Les membres du comité consultatif devraient posséder une expertise en matière de données et de technologie, d'éthique et de droits de la personne, de vie privée, de Te Ao Māori, de données Māori et de souveraineté des données et de politique publique (Police néo-zélandaise, 2021). Le comité comprend jusqu'à six membres indépendants (président inclus), qui sont nommés par le commissaire de police pour un mandat de plusieurs années. Un autre expert peut être amené à intervenir de façon ponctuelle lorsque des compétences supplémentaires particulières sont nécessaires. Les membres de ce comité sont admissibles à une rémunération (Police néo-zélandaise, 2021).

6.4 Poursuites

Les problèmes créés par les contraintes de capacité sont amplifiés par les délais constitutionnels de jugement des affaires criminelles

Les divers problèmes de capacité auxquels sont confrontées les forces de l'ordre, décrits à la section 6.2, deviennent des obstacles encore plus importants lorsqu'ils sont combinés aux contraintes du système judiciaire canadien. Notamment, la Cour suprême du Canada a imposé des délais maximums dans sa décision *R. c. Jordan* de 2016, qui a affirmé que le droit d'être jugé dans un délai raisonnable est garanti par la *Charte canadienne des droits et libertés*. La décision stipule que le temps entre l'arrestation d'un individu et son procès ne pouvait être supérieur à 18 mois dans les cours provinciales ou territoriales et à 30 mois dans les cours

supérieures (CSC, 2016b; JUS, 2019). Si ce délai est dépassé, les affaires criminelles peuvent être suspendues, sauf circonstances exceptionnelles — les procureurs peuvent faire valoir que les retards sont dus à des circonstances indépendantes de leur volonté (CSC, 2016b; JUS, 2019).

Les forces de l'ordre ont toutefois de la difficulté à recueillir et à analyser les preuves nécessaires dans ce délai (Cohen *et al.*, 2021). En outre, lorsque les affaires se retrouvent devant les tribunaux, elles sont plus complexes qu'autrefois et nécessitent plus de temps pour être menées à bien (JUS, 2019). L'effet global est que les ressources limitées peuvent être concentrées sur des crimes graves ou très médiatisés, de sorte que des actes cybercriminels plus courants ou moins graves ne font l'objet ni d'enquête ni de poursuites, en particulier dans les cas où toutes deux nécessitent des moyens importants. En effet, Cohen *et al.* (2021) expliquent que les enquêtes sur des crimes graves faisant appel à des preuves numériques manquent souvent de ressources policières et de personnel pour respecter les délais requis par l'*arrêt R. c. Jordan*. Cela signifie que, depuis cet arrêt, des centaines d'affaires concernant des crimes graves — tels que des meurtres, des agressions sexuelles et des infractions liées à la drogue — ont été suspendues (LCJC, 2017).

Le manque de personnel autre que dans les forces de l'ordre nuit à la capacité du système de justice pénale dans son ensemble à poursuivre les cybercrimes

Au sein du système judiciaire canadien, les contraintes de capacité de lutte contre la cybercriminalité dépassent les forces de l'ordre; ces contraintes ont été aggravées par la pandémie de COVID-19, qui a créé des arriérés supplémentaires et une augmentation des incidents de cybercriminalité (Nesbitt et Hansen, 2021). Le sous-financement, le manque de personnel, les données inadéquates et le trop faible nombre de juges de nomination fédérale sont quelques-uns des obstacles qui persistent (LCJC, 2017). En avril 2022, 58 postes de juge de nomination fédérale étaient vacants au Canada et des postes n'étaient pas pourvus dans 9 provinces ou territoires ainsi que dans des tribunaux fédéraux (CMF, 2022). Des pénuries de procureurs de la Couronne ont également été signalées dans plusieurs parties du pays (Taylor, 2017; Parsons, 2021). Le problème est particulièrement aigu en Alberta; selon un article de la CBC, le ministère de la Justice de la province a déclaré compter 47 postes non pourvus (sur un total de 378) au 30 septembre 2021 (Parsons, 2021). En novembre de la même année, l'Association des avocats de la Couronne de l'Alberta (Alberta Crown Attorneys' Association) a affirmé qu'environ 1 200 affaires de la cour provinciale risquaient d'être suspendues à cause de la pénurie (Parsons, 2021).

Il y a un manque de compétences numériques élémentaires dans l'ensemble du système de justice pénale

Le manque de compétences numériques élémentaires parmi les personnes travaillant dans le système de justice pénale, outre l'application de la loi, crée des obstacles à la poursuite des crimes cyberfacilités. Les procureurs et les juges au criminel ont généralement une expertise et une connaissance faibles dans les sujets touchant la cybercriminalité (Harkin et Whelan, 2019). Cela peut imposer une charge de travail plus lourde aux agents de police, qui doivent rédiger des rapports plus longs avec une mise en contexte et des explications supplémentaires particulières à la technologie (Watson et Huey, 2020). En outre, les justifications compliquées ou très techniques peuvent devenir un défi pour la défense, et rendre le coût de la contestation des preuves élevé ou prohibitif pour l'accusé. Les lacunes de compétences numériques exercent donc une pression supplémentaire sur un système dont les ressources sont déjà très limitées. Comme pour la police, la formation et l'amélioration des compétences en cybercriminalité peuvent être bénéfiques pour les procureurs et les juges (Dupont, 2021).

6.5 Résumé

Pour répondre à la question du commanditaire sur les défis posés par les progrès des technologies numériques et sur ce qu'ils signifient pour les enquêtes et les poursuites des crimes ou pour la lutte contre les préjudices en ligne, le comité d'experts a axé ce chapitre sur les difficultés auxquelles les forces de l'ordre sont confrontées sur le terrain lorsqu'elles appliquent les lois et les règlements en vigueur au Canada. Le comité a constaté que les principaux problèmes découlent de la structure organisationnelle des corps policiers, qui repose sur un modèle généraliste mal adapté au paysage moderne de l'application de la loi. Cette structure cause des lacunes importantes de connaissances et des difficultés à obtenir et à conserver les compétences numériques essentielles nécessaires pour enquêter sur le nombre croissant de crimes cyberfacilités signalés. Au-delà des compétences spécialisées, de nombreux agents généralistes ne possèdent pas les compétences numériques de base nécessaires pour faire face à la nature changeante de la criminalité à l'ère numérique.

Outre les problèmes de structure et de personnel, les forces de l'ordre sont confrontées à des défis pratiques dans les enquêtes criminelles et l'analyse des preuves numériques en raison des progrès technologiques. Il s'agit notamment de la difficulté à acquérir rapidement les renseignements numériques nécessaires, à contourner le chiffrement et à trouver des mécanismes permettant de détecter le matériel illégal parmi le contenu légal. Dans le même temps, bon nombre des technologies et réglementations mêmes qui compliquent l'acquisition ou l'analyse des données par les forces de l'ordre (p. ex. les ordonnances de communication,

le chiffrement) sont également essentielles à la protection de la sécurité publique et de la vie privée.

Le chapitre a également exposé plusieurs pratiques et certains outils émergents qui pourraient être utilisés au Canada pour relever certains des défis posés par les technologies numériques. Ces pratiques consistent notamment à renforcer la formation aux compétences numériques des personnes travaillant dans le système de justice pénale, mais aussi à faire évoluer le maintien de l'ordre vers une professionnalisation accrue, grâce à laquelle les agents pourront se spécialiser et être récompensés pour leurs compétences numériques de haut niveau ou pour l'amélioration de ces compétences. Il existe également des possibilités d'utiliser les technologies numériques pour prévenir et déceler (par la détection et le signalement) les crimes cyberfacilités et enquêter dessus. Chaque nouvelle technologie s'accompagne toutefois de facteurs éthiques qui lui sont propres, et son application sans orientation ou surveillance adéquate peut engendrer des atteintes à la vie privée ou aux droits de la personne contre les individus mêmes que la police est chargée de protéger. Ceci, à son tour, entrave davantage l'application de la loi en perpétuant une méfiance à l'égard de toute technologie ou nouvelle méthode. Le comité d'experts a conclu que, à l'avenir, une réglementation appropriée et une surveillance continue, la transparence et la responsabilité dans l'utilisation des nouvelles technologies ou des nouveaux modèles peuvent favoriser leur intégration et leur utilisation appropriées dans le domaine policier.

7

Réflexions du comité d'experts

La prolifération des technologies numériques en constante évolution pose des problèmes urgents pour la sécurité publique canadienne. Ces technologies sont omniprésentes dans la société et sont utilisées pour causer des préjudices importants à toutes les personnes vivant au Canada, même celles qui ne sont pas sur Internet ou qui utilisent rarement les TIC. Dans le même temps, les gens ne savent pas vers qui se tourner lorsqu'ils sont pris pour cible et n'ont pas accès aux ressources qui pourraient prévenir, atténuer ou réparer les dommages causés par les méfaits cyberfacilités. Le présent rapport met en lumière de nombreux cas où les approches adoptées par les différents ordres de gouvernement, par les forces de l'ordre et par le secteur privé ont été insuffisantes ou n'ont pas été adaptées pour relever les défis posés par l'évolution du paysage numérique.

Les lois nationales actuelles destinées à garantir la sécurité publique et à offrir des recours aux victimes et aux survivants d'actes préjudiciables sont souvent insuffisantes lorsqu'il s'agit de répondre à des menaces et des méfaits en constante évolution. Le droit criminel, la responsabilité délictuelle, le droit civil du Québec et la législation fédérale sur la protection des renseignements personnels offrent un ensemble de mécanismes disparates, mais aucun ne répond pleinement à la nécessité de renforcer le contrôle des individus sur leurs données ou ne leur donne l'accès rapide à des recours efficaces. En outre, tous les méfaits cyberfacilités ne peuvent ou ne doivent pas être traités par des règles sanctionnées par l'État. Certains requièrent une démarche multidimensionnelle fondée sur le soutien communautaire, les programmes éducatifs et la responsabilité sociale des entreprises.

Les gouvernements du monde entier ont entrepris des réformes juridiques pour renforcer la sécurité publique dans un contexte numérique. Le présent rapport a examiné un éventail de politiques mises en œuvre et proposées dans des pays qui présentent des similitudes sociopolitiques avec le Canada et qui sont liés à ce dernier par des relations diplomatiques étroites, à savoir l'Australie, l'Allemagne, la Nouvelle-Zélande, le Royaume-Uni, les États-Unis et l'Union européenne. Ces réformes criminalisent certains méfaits en ligne, étendent la portée réglementaire de l'État administratif aux espaces numériques, accélèrent le retrait de certains éléments de contenu et réforment les exigences en matière de consentement au traitement des données, entre autres. Certaines mesures encouragent toutefois une plus grande surveillance du discours et des utilisateurs sur Internet, entraînant la suppression de contenu légal et suscitant ainsi des inquiétudes quant à la liberté d'expression et au respect de la vie privée.

Si les décideurs canadiens peuvent tirer des leçons de l'expérience étrangère, tous les ordres de gouvernement doivent tenir compte du contexte juridique et social canadien lorsqu'ils évaluent l'applicabilité des approches étrangères aux questions

nationales. Par exemple, contrairement au Canada, l'Australie n'a pas de déclaration des droits inscrite dans la constitution, tandis que la politique numérique des États-Unis met l'accent sur la protection de la liberté d'expression en vertu du premier amendement de la *Constitution des États-Unis*. Ces difficultés juridiques sont exacerbées par le fait que tous les méfaits en ligne n'atteignent pas le seuil du comportement illégal. Si une réforme juridique peut s'avérer nécessaire pour remédier à certains méfaits sur le Web, dans d'autres cas, des mesures politiques différentes seront plus efficaces pour prévenir et régler ces méfaits et répondre aux besoins des victimes et des survivants.

Certains méfaits cyberfacilités qui enfreignent le droit criminel sont des crimes facilités par les TIC. Ce rapport a démontré que l'application de la sécurité publique numérique se heurte à un ensemble de défis qui lui sont propres en matière de prévention, d'enquêtes, d'analyse et de poursuite des crimes cyberfacilités. Le comité d'experts a déterminé que le volume des données, le manque de ressources et les lacunes de compétences, ainsi que des structures organisationnelles dépassées, sont les principaux obstacles à l'efficacité du travail des forces de l'ordre. L'amélioration des compétences numériques des personnes travaillant dans l'ensemble du système de justice pénale, l'élaboration de réformes permettant aux agents possédant des compétences numériques spécialisées de progresser dans la hiérarchie tout en continuant à développer et à appliquer ces compétences et la professionnalisation accrue des services de police peuvent aider les États à surmonter certains des défis créés par la nature changeante de la criminalité au Canada. Il existe également toute une série de technologies numériques qui peuvent être employées pour faciliter la détection, la prévention et l'investigation des crimes cyberfacilités. La réglementation, la transparence et la surveillance sont toutefois essentielles pour garantir que toute technologie ou tout modèle adopté respecte certaines normes en matière d'éthique et de droits de la personne lorsqu'il est intégré et utilisé pour l'application de la loi.

Enfin, l'intervention publique ne peut à elle seule améliorer la santé globale de l'écosystème numérique. Les organisations du secteur privé, et les platesformes de médias sociaux sur Internet en particulier, jouent un rôle important à cet égard. Même si des entreprises déploient des efforts volontaires pour limiter la prolifération du contenu préjudiciable, le contenu en ligne se répand rapidement sur différentes platesformes dans le monde entier, défiant les mesures de modération du contenu. En outre, dans la mesure où le contenu incendiaire suscite la réaction des utilisateurs, les platesformes ne sont pas incitées à introduire des réformes qui modifieraient considérablement leur modèle d'autorégulation.

Dans le domaine de la sécurité publique numérique, les problèmes de gouvernance sont exacerbés par le fait que les initiatives publiques et privées de détection et de prévention des cyberméfaits considèrent souvent à tort que vie privée et sécurité

sont contradictoires. Selon le comité d'experts, la sécurité et la vie privée peuvent se renforcer mutuellement — ce qui signifie que les mesures de renforcement de la sécurité ne doivent pas minimiser les importantes protections de la vie privée, telles que la capacité des individus à contrôler qui a accès à leurs données, quand et dans quel but.

Le rapport du comité d'experts souligne les problèmes imminents que posent les technologies numériques en matière de vie privée et de sécurité et la nécessité urgente de s'attaquer à ces problèmes, tout en tenant compte des questions sociales et juridiques complexes qui sous-tendent la sécurité publique numérique. De plus, les technologies numériques présentent des défis importants en matière de sécurité publique, qui dépassent les frontières nationales, des défis qui ne feront qu'augmenter avec l'arrivée de nouvelles technologies sur le marché. Toutefois, des réformes de portée et d'ampleur variables pour mieux assurer la sécurité publique numérique sont envisageables. La promotion d'un écosystème numérique plus sûr est un effort collectif qui doit réunir la société civile, les décideurs, les forces de l'ordre et le secteur privé — et qui repose sur la coopération internationale ainsi que sur des approches juridiques et non juridiques guidées par l'expérience des victimes et des survivants.

Références

Aaronson, S. A. et P. Leblond, 2018. « Another digital divide: The rise of data realms and its implications for the WTO », *Journal of International Economic Law*, vol. 21, n°2, p. 245-272.

AARP, 2022. Cryptocurrency Fraud. Adresse : https://www.aarp.org/money/scams-fraud/info-2019/cryptocurrency.html (consulté en mars 2022).

Abacus Data, 2021. *Online Hate and Racism Canadian Experiences and Opinions on What to Do About It*, Ottawa, ON, Abacus Data.

ABCA, Alberta Court of Appeal, 2022. *R. v. Bykovets*, Calgary, AB, Alberta Court of Appeal.

Abreu, R. L. et M. C. Kenny, 2018. « Cyberbullying and LGBTQ youth: A systematic literature review and recommendations for prevention and intervention », *Journal of Child and Adolescent Trauma*, vol. 11, n°1, p. 81-97.

ACCP – Association canadienne des chefs de police, 2016. *Résolutions adoptées à la 111e Conférence annuelle*, Ottawa, ON, ACCP.

ACFC – Agence de la consommation en matière financière du Canada, 2019. Transactions par carte de crédit et de débit non autorisées : connaissez vos droits et responsabilités. Adresse : https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/droits-responsabilites/protection-transactions-non-autorisees.html (consulté en mai 2022).

ACVM – Autorités Canadiennes en valeurs mobilières, 2020. *ACVM Staff Notice 21-327: Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets*, Ottawa, ON, ACVM.

ACVM et OCRCVM – Autorités Canadiennes en valeurs mobilières et Organisme canadien de réglementation du commerce des valeurs mobilières, 2021. Avis conjoint 21-329 du personnel des Autorités canadiennes en valeurs mobilières et de l'Organisme canadien de réglementation du commecerce de valeurs mobilières *: Indications à l'intention des plateformes de négociation de cryptoactifs : Conformité aux obligations réglementaires*, Ottawa, ON, ACVM et OCRCVM.

Adee, S., 2020. What Are Deepfakes and How Are They Created? Adresse : https://spectrum.ieee.org/what-is-deepfake (consulté en janvier 2022).

AFAC – L'Association des femmes autochtones du Canada, 2014. *Sexual Exploitation and Trafficking of Aboriginal Women and Girls: Literature Review and Key Informant Interviews*, Gatineau, QC, AFAC.

Agrafiotis, I., J. R. Nurse, M. Goldsmith, S. Creese, et D. Upton, 2018. « A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate », *Journal of Cybersecurity*, vol. 4, n°1, p. 1-15.

Ahmad, H., 2017. « Youth de-radicalization: A Canadian framework », *Journal for Deradicalization*, n°12, p. 119-168.

AHRC – Australian Human Rights Commission, s.d. How are Human Rights Protected in Australian Law? Adresse : https://humanrights.gov.au/our-work/rights-and-freedoms/how-are-human-rights-protected-australian-law (consulté en janvier 2022).

Ajder, H., G. Patrini, F. Cavalli, et L. Cullen, 2019. *The State of Deepfakes: Landscape, Threats, and Impact*, Amsterdam, Netherlands, Deeptrace.

Al-Khateeb, H. M., G. Epiphaniou, Z. A. Alhaboby, J. Barnes, et E. Short, 2017. « Cyberstalking: Investigating formal intervention and the role of corporate social responsibility », *Telematics and Informatics*, vol. 34, n°4, p. 339-349.

Al-Qazzaz, K., 2020. Islamophobia is on the Rise During COVID-19. Adresse : https://policyoptions.irpp.org/magazines/october-2020/islamophobia-is-on-the-rise-during-covid-19/ (consulté en décembre 2022).

Alavi, S., E. Charleston, S. Du Perron, D.-N. El-Khoury, B. Freedman, J. Gauthier, … D. Windt, 2022. *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for Businesses*, Toronto, ON, Borden Ladner Gervais LLP.

Albin-Lackey, C., 2013. *Without Rules: A Failed Approach to Corporate Accountability*, New York, NY, Human Rights Watch.

Albu, O. B. et M. Flyverbom, 2016. « Organizational Transparency: Conceptualizations, Conditions, and Consequences », *Business & Society*, vol. 58, n°2, p. 268-297.

Alexander, J., 2015. *How Technology is Killing Privacy*, Allendale, MI, Grand Valley State University.

Alkhalil, Z., C. Hewage, L. Nawaf, et I. Khan, 2021. « Phishing attacks: A recent comprehensive study and a new anatomy », *Frontiers in Computer Science*, vol. 3, 563060.

AlKhatib, B. et R. Basheer, 2019. « Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation », *Journal of Digital Information Management*, vol. 17, n°2, p. 51.

Allen & Overy, 2020. The Digital Services Act Package Is Here. Adresse : https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-digital-services-act-package-is-here (consulté en avril 2020).

Allen, B., 2019. Revenge Porn and Sext Crimes: Canada Sees More than 5,000 Police Cases as Law Marks 5 Years. Adresse : https://www.cbc.ca/news/canada/saskatchewan/revenge-porn-and-sext-crimes-canada-sees-more-than-5-000-police-cases-as-law-marks-5-years-1.5405118 (consulté en novembre 2021).

Andrey, S., A. Rand, M. J. Masoodi, et S. Tran, 2021a. *Private Messaging Public Harms: Disinformation and Online Harms on Private Messaging Platforms in Canada*, Toronto, ON, Ryerson University.

Andrey, S., A. Rand, M. J. Masoodi, et K. Bardeesy, 2021b. *Rebuilding Canada's Public Square*, Toronto, ON, Ryerson University.

Appel de Christchurch, 2019. Appel à l'action de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne. Adresse : https://www.christchurchcall.com/assets/Documents/Appel-de-Christchurch-texte-complet-francais.pdf (consulté en juillet 2021).

Appel de Christchurch, 2021. *Consultation des soutiens de l'appel de Christchurch: Rapport final*, Wellington, Nouvelle-Zélande, Appel de Christchurch.

Apple, 2022. An Update on AirTag and Unwanted Tracking. Adresse : https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/ (consulté en avril 2022).

Aquilina, K., 2010. « Public security versus privacy in technology law: A balancing act? », *Computer Law & Security Review*, vol. 26, p. 130-143.

ARC – Agence du revenu du Canada, 2021. Guide de la monnaie virtuelle pour les utilisateurs de cryptomonnaie et les professionnels de l'impôt. Adresse : https://www.canada.ca/fr/agence-revenu/programmes/a-propos-agence-revenu-canada-arc/observation/monnaie-numerique/cryptomonnaies-guide.html (consulté en février 2022).

Ardill, L., 2021. Know the Facts: TikTok's Latest Move Against Misinformation. Adresse : https://www.siliconrepublic.com/companies/tiktok-know-the-facts-new-fact-checking-feature (consulté en juin 2021).

ASIO, Australian Security Intelligence Organisation, 2021. *ASIO Annual Report 2020-21*, Canberra, Australie, Gouv. de l' Australie.

Askanius, T., 2021. « On frogs, monkeys, and execution memes: Exploring the humor-hate nexus at the intersection of neo-Nazi and alt-right movements in Sweden », *Television & New Media*, vol. 22, n°2, p. 147-165.

ASPC – Agence de la santé publique du Canada, 2019. *Canada : un pays pionnier. Feuille de route du Canada pour mettre fin à la violence à l'égard des enfants*, Ottawa, ON, ASPC.

Austin, L., 2012. *Privacy, Shame and the Anxieties of Identity*, Toronto, ON, University of Toronto.

AUSTRAC – Australian Transaction Reports and Analysis Centre, 2018. New Australian Laws to Regulate Cryptocurrency Providers. Adresse : https://www.austrac.gov.au/new-australian-laws-regulate-cryptocurrency-providers (consulté en février 2022).

Awan, I. et I. Zempi, 2015. *We Fear for our Lives: Offline and Online Experiences of Anti-Muslim Hostility*, United Kingdom, Tell MAMA, Birmingham City University, Nottingham Trent University.

Badour, A., S. Shah, et E. Berg, 2020. FINTRAC Guidance on Red Flag Indicators Associated With Virtual Currency Transactions. Adresse : https://www.mccarthy.ca/fr/node/68556 (consulté en avril 2022).

Bailey, J., 2008. « Towards an equality-enhancing conception of privacy », *The Dalhousie Law Journal*, vol. 31, n°2, p. 267-309.

Bailey, J., 2015. « A Perfect Storm: How the Online Environment, Social Norms, and Law Shape Girls' Lives », dans Bailey, J. et V. Steeves(réd.), *eGirls, eCitizens*, Ottawa, ON, University of Ottawa Press.

Bailey, J. et S. Shayan, 2016. « Missing and murdered Indigenous women crisis: Technological dimensions », *Canadian Journal of Women and the Law*, vol. 28, n°2, p. 321-341.

Bailey, J., V. Steeves, et S. Dunn, 2017. *Submission to the Special Rapporteur on Violence Against Women, Re: Regulating Online Violence and Harassment Against Women*, Ottawa, ON, University of Ottawa.

Bailey, J. et C. Mathen, 2019. « Technology-facilitated violence against women & girls: Assessing the Canadian criminal law response », *Canadian Bar Review*, vol. 97, n°3, p. 664-696.

Baird, K., K. P. McDonald, et J. Connolly, 2020. « Sex trafficking of women and girls in a southern Ontario region: Police file review exploring victim characteristics, trafficking experiences, and the intersection with child welfare », *Canadian Journal of Behavioural Science/Revue canadienne des sciences du comportement*, vol. 52, n°1, p. 8-17.

Balkin, J., 2009. « The future of free expression in a digital age », *Pepperdine Law Review*, vol. 36, n°2, p. 427-444.

Ballard, B. et C. Parsons, 2022. « Mixed traditions: Evaluating telecommunications transparency », *Internet Policy Review*, vol. 11, n°1, p. 1-30.

Bambauer, D. E., 2013. « Privacy versus security », *Journal of Criminal Law and Criminology*, vol. 103, n°3, p. 667-684.

Bankston, K. S. et A. Soltani, 2014. « Tiny constables and the cost of surveillance: Making cents out of United States v. Jones », *The Yale Law Journal Online*, vol. 123, p. 335-357.

Baril, D. E., 2014. *La transformation des enquêtes policières due à l'influence des technologies : perspective d'une unité policière spécialisée en analyse judiciaire informatique*, Montréal, QC, Université de Montréal.

Barocas, S. et A. D. Selbst, 2016. « Big data's disparate impact », *California Law Review*, vol. 104, n°3, p. 671-732.

Baron, J., A. O'Mahony, D. Manheim, et C. Dion-Schwarz, 2015. *National Security Implications of Virtual Currency*, Santa Monica, CA, RAND Corporation.

Bastug, M. F., A. Douai, et D. Akca, 2020. « Exploring the "demand side" of online radicalization: Evidence from the Canadian context », *Studies in Conflict & Terrorism*, vol. 43, n°7, p. 616-637.

BBC News, 2021. Twitter Suspends 70,000 Accounts Linked to QAnon. Adresse : https://www.bbc.com/news/technology-55638558 (consulté en juin 2021).

BCIT – British Columbia Institute of Technology, s.d. Forensic Investigation. Adresse : https://www.bcit.ca/programs/forensic-investigation-digital-forensics-and-cybersecurity-option-bachelor-of-technology-full-time-part-time-845jbtech/#overview (consulté en janvier 2022).

BCPC – Provincial Court of British Columbia, 2012. *R. v. Corby 2012 BCPC 561*, Vancouver, BC, BCPC.

BDC – La Banque de développement du Canada, 2022. Sociofinancement. Adresse : https://www.bdc.ca/fr/articles-outils/boite-outils-entrepreneur/gabarits-documents-guides-affaires/glossaire/sociofinancement. (consulté en avril 2022).

Beaulac, S. et J.-F. Gaudreault-DesBiens, 2017. *Droit civil et common law: convergences et divergences*, Ottawa, ON, Fédération des ordres professionnels de juristes du Canada.

Becker, M., 2019. « Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy », *Ethics and Information Technology*, vol. 21, p. 301-317.

Beesley, P., 2021. *Competency-Based Management Framework for Digital Competencies in Canadian Policing*, Charlottetown, PE, Canadian Police Knowledge Network.

Bell, S., 2020. « CSIS Warns about Conspiracy Theories Linking COVID-19 to 5G Technology ». *Global News* (3 décembre).

Bellemare, A. et J. Ho, 2020. Social Media Firms Catching More Misinformation, But Critics Say 'They Could Be Doing More'. Adresse : https://www.cbc.ca/news/science/social-media-platforms-pandemic-moderation-1.5536594 (consulté en novembre 2021).

Bellemare, A., J. Ho, et K. Nicholson, 2020. Quebec Police Investigating Possible Link between Cell Tower Fires and 5G Coronavirus Conspiracy Theories. Adresse : https://www.cbc.ca/news/canada/coronavirus-conspiracy-theory-5g-fires-quebec-1.5560570 (consulté en décembre 2022).

Bellman, S., E. J. Johnson, S. J. Kobrin, et G. L. Lohse, 2004. « International differences in information privacy concerns: A global survey of consumers », *The Information Society*, vol. 20, n°5, p. 313-324.

Bellovin, S. M., M. Blaze, S. Clark, et L. Susan Landau, 2014. « Lawful hacking: Using existing vulnerabilities for wiretapping on the internet », *Northwestern Journal of Technology and Intellectual Property*, vol. 12, n°1, article 1.

Benesch, S., D. Ruths, K. P. Dillon, H. M. Saleem, et L. Wright, 2016. *Counterspeech on Twitter: A Field Study*, Ottawa, ON, Kanishka Project, Public Safety Canada.

Benkler, Y., R. Faris, et H. Roberts, 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York, NY, Oxford University Press.

Bennett, C. J. et C. D. Raab, 2018. *The Governance of Privacy: Policy Instruments in Global Perspective*. New York, NY, Routledge.

Bennett Jones, 2021. Changes to AML and Virtual Currency Regulations for Reporting Entities and Money Service Businesses. Adresse : https://www4.bennettjones.com/Blogs-Section/Changes-to-AML-and-Virtual-Currency-Regulations-for-Reporting-Entities-and-Money-Service-Businesses#:~:text=Entities%20dealing%20in%20%22virtual%20currencies%22%2C%20money%20services%20businesses,regulations%20come%20into%20force%20June%201%2C%202021.%201 (consulté en avril 2022).

Bennett Moses, L., 2007. « Recurring dilemmas: Law's race to keep up with technological change », *Journal of Law, Technology & Policy*, vol. 2007, n°2, p. 239-285.

Bennett, W. L. et S. Livingston, 2020. « Conclusion - Defending Democracy in the Disinformation Age », dans Bennett, W. L. et S. Livingston(réd.), *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States*, New York, NY, Cambridge University Press.

Berentsen, A. et F. Schär, 2018. « A short introduction to the world of cryptocurrencies », *Federal Reserve Bank of St. Louis Review*, vol. 100, n°1, p. 1-16.

Berger, J. M., 2019. The Dangerous Spread of Extremist Manifestos. Adresse : https://www.theatlantic.com/ideas/archive/2019/02/christopher-hasson-was-inspired-breivik-manifesto/583567/ (consulté en mai 2022).

Bernaciak, C. et D. Ross, 2022. How Easy Is It to Make and Detect a Deepfake? Adresse : https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/ (consulté en octobre 2022).

Berners-Lee, T., 2019. I Invented the World Wide Web. Here's How We Can Fix It. Adresse : https://www.nytimes.com/2019/11/24/opinion/world-wide-web.html (consulté en décembre 2022).

Bernier, C., 2012. *The Integral Role of Civil Society in Balancing Privacy and National Security*, communication présentée dans le cadre du International Intelligence Review Agencies Conference, Ottawa, ON.

Bessi, A., F. Petroni, M. Del Vicario, F. Zollo, A. Anagnostopoulos, A. Scala, ... W. Quattrociocchi, 2016. « Homophily and polarization in the age of misinformation », *The European Physical Journal Special Topics*, vol. 225, n°10, p. 2047-2059.

Beswick, S., 2022. *Tort Law: Cases and Commentaries (2nd ed.)*. Vancouver, BC, University of British Columbia.

Bhullar, R., 2022. Online Streaming Act Bill C-11 Repeats Bill C-10's Mistakes. Adresse : https://openmedia.org/article/item/online-streaming-act-bill-c-11-repeats-bill-c-10s-mistakes (consulté en avril 2022).

Bidgoli, M. et J. Grossklags, 2016. *End User Cybercrime Reporting: What We Know and What We Can Do to Improve It*, communication présentée dans le cadre du 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC.

Binns, C. A. et R. J. Kempf, 2021. « Who Has Legal Responsibility for Safety and Security in Hotels Versus Home Sharing? », dans Binns, C. A. et R. J. Kempf(réd.), *Safety and Security in Hotels and Home Sharing*, Cham Switzerland, Springer.

Bitwise Asset Management, 2019. *Bitwise Asset Management - Presentation to the U.S. Securities and Exchange Commission*, Washington, DC, Bitwise Asset Management.

BLG – Borden Ladner Gervais, 2021. *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, Montréal QC, BLG.

Blumenfeld, W. J. et R. M. Cooper, 2010. « LGBT and allied youth responses to cyberbullying: Policy implications », *International Journal of Critical Pedagogy*, vol. 3, n°1, p. 114-133.

Bohannon, M., 2018. The State of Encryption: How the Debate Has Shifted. Adresse : https://opensource.com/article/18/6/listening-susan-landau (consulté en mars 2022).

Bond, S., 2021. Unwelcome on Facebook and Twitter, QAnon Followers Flock to Fringe Sites. Adresse : https://www.npr.org/2021/01/31/962104747/unwelcome-on-facebook-twitter-qanon-followers-flock-to-fringe-sites (consulté en novembre 2021).

Booker, B., 2021. Facebook Removes 'Stop The Steal' Content; Twitter Suspends QAnon Accounts. Adresse : https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/12/956003580/facebook-removes-stop-the-steal-content-twitter-suspends-qanon-accounts (consulté en juin 2021).

Bossler, A. M. et T. J. Holt, 2012. « Patrol officers' perceived role in responding to cybercrime », *Policing: An International Journal of Police Strategies & Management*, vol. 35, n°1, p. 165-181.

Bothamley, S. et R. J. Tully, 2018. « Understanding revenge pornography: Public perceptions of revenge pornography and victim blaming », *Journal of Aggression Conflict and Peace Research*, vol. 10, n°1, p. 1-10.

Boutilier, A., 2016. Encryption Creating a Barrier for Police, Documents Suggest. Adresse : https://www.thestar.com/news/canada/2016/07/02/encryption-creating-a-barrier-for-police-documents-suggest.html (consulté en mars 2022).

Boutilier, A. et J. Ling, 2020. Canadian Forces Reservist Who Stormed Rideau Hall Grounds Faces 22 Charges. Adresse : https://www.thestar.com/politics/federal/2020/07/03/rcmp-release-new-details-of-armed-man-who-gained-access-to-rideau-hall-grounds-thursday.html (consulté en décembre 2022).

Boutin-Clermont, M.-A., 2014. Chronique - La Criminalisation du « revenge porn » : Entre Théorie et Pratique. Adresse : https://www.editionsyvonblais.com/blogue/marie-andree-boutin-clermont/chronique-la-criminalisation-du-revenge-porn-entre-theorie-et-pratique-30/ (consulté en mai 2022).

Braga, M., 2017. Facial Recognition Technology is Coming to Canadian Airports This Spring. Adresse : https://www.cbc.ca/news/science/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344 (consulté en avril 2022).

Brannon, V. C., 2019. *Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230*, Washington, DC, Congressional Research Service.

Brennen, J. S., F. M. Simon, et R. K. Nielsen, 2021. « Beyond (mis)representation: Visuals in COVID-19 misinformation », *The International Journal of Press/Politics*, vol. 26, n°1, p. 277-299.

Brey, P., 2017. « Theorizing Technology and its Role in Crime and Law Enforcement », dans McGuire, M. R. et T. J. Holt(réd.), *The Routledge Handbook of Technology, Crime and Justice*, Abingdon, United Kingdom, Routledge.

Brideau, I. et L. Brosseau, 2019. *The Distribution of Legislative Powers: An Overview*, Ottawa, ON, Library of Parliament.

Brideau, I., G. de Billy Brown, F. Lord, et M. Ménard, 2020. *Bill C-10: An Act to Amend the Broadcasting Act and to Make Related and Consequential Amendments to Other Acts*, Ottawa, ON, Library of Parliament.

Bridgman, A., E. Merkley, O. Zhilin, P. J. Loewen, T. Owen, et D. Ruths, 2021. « Infodemic pathways: Evaluating the role that traditional and social media play in cross-national information transfer », *Frontiers in Political Science*, vol. 3, 648646.

Bridgman, A., M. Lavigne, M. Baker, T. Bergeron, D. Bohonos, A. Burton, … P. Loewen, 2022. *Mis- and Disinformation During the 2021 Canadian Federal Election*, Montréal, QC, Media Ecosystem Observatory.

Brighton, M., 2004. BT Puts Block on Child Porn Sites. Adresse : https://www.theguardian.com/technology/2004/jun/06/childrensservices.childprotection (consulté en février 2022).

Broll, R. et L. Huey, 2015. « «Just being mean to somebody isn't a police matter»: Police perspectives on policing cyberbullying », *Journal of School Violence*, vol. 14, n°2, p. 155-176.

Broll, R., C. Dunlop, et C. V. Crooks, 2018. « Cyberbullying and internalizing difficulties among Indigenous adolescents in Canada: Beyond the effect of traditional bullying », *Journal of Child & Adolescent Trauma*, vol. 11, n°1, p. 71-79.

Brookes, J., 2022. Big Tech Says it is Confused by Australia's Growing Online Safety Laws. Adresse : https://www.innovationaus.com/big-tech-says-it-is-confused-by-australias-growing-online-safety-laws/ (consulté en janvier 2022).

Brown, A., M. Gibson, et E. Short, 2017. « Modes of cyberstalking and cyberharassment: Measuring the negative effects in the lives of victims in the UK », *Annual Review of Cybertherapy and Telemedicine*, n°15, p. 57-63.

Browning, K., 2021. « Extremists Find a Financial Lifeline on Twitch ». *The New York Times* (27 avril).

Brownsword, R., 2008. *Rights, Regulation, and the Technological Revolution*. Oxford, Royaume-Uni, Oxford University Press.

Brugoni, M., 2018. « Le e-learning cybercrime : une formation harmonisée », *POLCANT info*, vol. 109, p. 12-13.

Bull, M., 2021. Exclusive: What is data poisoning and why should we be concerned? Adresse : https://internationalsecurityjournal.com/what-is-data-poisoning/ (consulté en mai 2022).

Buolamwini, J. et T. Gebru, 2018. « Gender shades: Intersectional accuracy disparities in commercial gender classification », *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, vol. 81, p. 77-91.

Burns, C. M., J. Morley, R. Bradshaw, et J. Domene, 2008. « The emotional impact on and coping strategies employed by police teams investigating internet child exploitation », *Traumatology*, vol. 14, n°2, p. 20-31.

Burruss, G., C. J. Howell, A. Bossler, et T. J. Holt, 2020. « Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis », *Policing: An International Journal*, vol. 43, n°1, p. 105-119.

Bygrave, A. L., 2010. « Privacy and data protection in an international perspective », *Scandinavian Studies in Law*, vol. 56, p. 165-200.

CAC – Conseil des académies canadiennes, 2014. *Le maintien de l'ordre au Canada au XXIe siècle : Une nouvelle police pour de nouveaux défis. Comité d'experts sur l'avenir des modèles canadiens de maintien de l'ordre*, Ottawa, ON, CAC.

CAC – Conseil des académies canadiennes, 2021. *En attente de connexion : Le comité d'experts sur les réseaux à haut débit pour les collectivités rurales et éloignées du Canada*, Ottawa, ON, CAC.

CAC – Conseil des académies canadiennes, 2022. *Entre progrès et défis : Le comité d'experts sur l'intelligence artificielle en sciences et en génie*, Ottawa, ON, CAC.

CAFC – Centre antifraude du Canada, 2020. Fraude téléphonique. Adresse : https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/telephone-telephonique-fra.htm (consulté en février 2022).

CAFC – Centre antifraude du Canada, 2021a. Signaler les cas de fraude et de cybercriminalité. Adresse : https://www.antifraudcentre-centreantifraude.ca/report-signalez-fra.htm (consulté en janvier 2021).

CAFC – Centre antifraude du Canada, 2021b. Les 10 fraudes ciblant les Canadiens les plus signalées en 2020. Adresse : https://www.antifraudcentre-centreantifraude.ca/features-vedette/2021/frauds-10-fraudes-fra.htm (consulté en novembre 2021).

CAFC – Centre antifraude du Canada, 2021c. Centre antifraude du Canada (Fraudes récentes). Adresse : https://www.antifraudcentre-centreantifraude.ca/index-fra.htm (consulté en novembre 2021).

CAFC – Centre antifraude du Canada, 2021d. Alerte à la fraude! Adresse : https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/service-fra.htm (consulté en novembre 2021).

Campbell, R. et J. Lovenduski, 2016. *Footprints in the Sand: Five Years of the Fabian Women's Network Mentoring and Political Education Programme*, Londres, Royaume-Uni, Fabian Society.

CANAFE – Centre d'analyse des opérations et déclarations financières du Canada, 2021a. *Canadiens en sécurité, économie sûre : Rapport annuel de 2020-2021*, Ottawa, ON, CANAFE.

CANAFE – Centre d'analyse des opérations et déclarations financières du Canada, 2021b. Qu'est-ce qu'une déclaration d'opérations douteuses? Adresse : https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-fra (consulté en août 2022).

CANAFE – Centre d'analyse des opérations et déclarations financières du Canada, 2021c. Indicateurs de blanchiment d'argent et de financement du terrorisme – Opérations en monnaie virtuelle. Adresse : https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-fra (consulté en mars 2022).

CANAFE – Centre d'analyse des opérations et déclarations financières du Canada, 2022. Mandat. Adresse : https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-fra (consulté en mars 2022).

Caneppele, S. et M. F. Aebi, 2019. « Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes », *Policing: A Journal of Policy and Practice*, vol. 13, n°1, p. 66-79.

Carbert, M., 2022. Liberals Re-Introduce Broadcasting Act Bill, Pledge Amendments Will Ensure Individual Social Media Users Are Exempt. Adresse : https://www.theglobeandmail.com/politics/article-liberals-re-introduce-broadcasting-act-bill-pledge-amendments-will/ (consulté en février 2022).

Carlini, N. et H. Farid, 2020. Evading deepfake-image detectors with white- and black-box attacks. Adresse : https://arxiv.org/pdf/2004.00622.pdf (consulté en août 2022).

Carter, W. A. et J. C. Daskal, 2018. *Low-Hanging Fruit*, Washington, DC, Center for Strategic & International Studies.

Carvin, S., T. Juneau, C. Forcese, et J. Pyrik, 2021a. « The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) », dans, *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, Toronto, ON, University of Toronto Press.

Carvin, S., T. Juneau, et C. Forcese, 2021b. « Conclusion », dans Carvin, S., T. Juneau et C. Forcese(réd.), *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, Toronto, ON, University of Toronto Press.

CBA – Association des banquiers canadiens, 2022. Fiche info - Protéger les Canadiens de la fraude. Adresse : https://cba.ca/protecting-canadians-from-fraud?l=fr (consulté en mai 2022).

CCADE – Assemblée citoyenne Canadienne sur l'expression démocratique, 2021. *Assemblée citoyenne Canadienne sur l'expression démocratique : Recommandations pour renforcer la capacité d'intervention du Canada face aux nouvelles technologies numériques et réduire les préjudices causés par leur mauvaise utilisation*, Ottawa, ON, Forum des politiques publiques.

CCECPV – Centre canadien d'engagement communautaire et de prévention de la violence, 2018. *Stratégie nationale de lutte contre la radicalisation menant à la violence*, Ottawa, ON, gouvernement du Canada.

CCPE – Centre canadien de protection de l'enfance, 2016. *Les images d'abus pédosexuels sur internet : Une analyse de Cyberaide.ca*, Winnipeg, MB, CCPE.

CCPE – Centre canadien de protection de l'enfance, 2017. *Cyberaide.ca: Rapport 15e anniversaire*, Winnipeg, MB, CCPE.

CCPE – Centre canadien de protection de l'enfance, 2021. *Project Arachnid : L'accessibilité des images d'abus pédosexuels sur internet*, Winnipeg, MB, CCPE.

CCSJSC – Centre canadien de la statistique juridique et de la sécurité des collectivités, 2021. *Manuel du Programme de déclaration uniforme de la criminalité (DUC)*, Ottawa, ON, Statistique Canada.

CdE – Conseil de l'Europe, 2021a. *Les avantages de l'adhésion à la Convention de Budapest sur la cybercriminalité*, Strasbourg, France, CdE.

CdE – Conseil de l'Europe, 2021b. Détails du traité n°189. Adresse : https://www.coe.int/fr/web/conventions/full-list2?module=treaty-detail&treatynum=189 (consulté en janvier 2022).

CdE – Conseil de l'Europe, 2021c. Nouveau traités. Adresse : https://www.coe.int/en/web/conventions/new-treaties (consulté en janvier 2022).

CdE – Conseil de l'Europe, 2022. Etat des signatures et ratifications du traité 185. Adresse : https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (consulté en octobre 2022).

CdE – Conseil de l'Europe, s.d.-a. La Convention de Budapest et ses protocoles. Adresse : https://www.coe.int/fr/web/cybercrime/the-budapest-convention (consulté en janvier 2022).

CdE – Conseil de l'Europe, s.d.-b. Convention de Budapest. Adresse : https://www.coe.int/fr/web/impact-convention-human-rights/convention-on-cybercrime#/ (consulté en octobre 2022).

CDH –Conseil des droits de l'homme des Nations Unies, 2011a. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, Genève, Suisse, ONU.

CDH –Conseil des droits de l'homme des Nations Unies, 2011b. *Principes directeurs relatifs aux entreprises et aux droits de l'homme mise en œuvre du cadre de référence «protéger, respecter et réparer» des Nations Unies*, Genève, Suisse, ONU.

CDO – Commission du droit de l'Ontario, 2020. *Defamation Law in the Internet Age*, Toronto, ON, CDO.

CDPDJ – Commission des droits de la personne et des droits de la jeunesse, 2022. L'exploitation. Adresse : https://cdpdj.qc.ca/fr/vos-obligations/ce-qui-est-interdit/lexploitation (consulté en janvier 2022).

Centre canadien pour la cybersécurité, 2020a. *Évaluation des cybermenaces nationales 2020*, Ottawa, ON, Centre de la sécurité des télécommunications.

Centre canadien pour la cybersécurité, 2020b. Faux comptes de médias sociaux. Adresse : https://cyber.gc.ca/fr/orientation/faux-comptes-de-medias-sociaux (consulté en février 2022).

Centre canadien pour la cybersécurité, 2021a. Introduction à l'environnement de cybermenace. Adresse : https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces (consulté en août 2022).

Centre canadien pour la cybersécurité, 2021b. *Bulletin sur les cybermenaces : La menace des rançongiciels en 2021*, Ottawa, ON, Centre de la sécurité des télécommunications.

Centre canadien pour la cybersécurité, 2022a. *Évaluation des cybermenaces nationales 2023-2024*, Ottawa, ON, Centre de la sécurité des télécommunications.

Centre canadien pour la cybersécurité, 2022b. *Repérer les cas de mésinformation, désinformation et malinformation*, Ottawa, ON, Centre de la sécurité des télécommunications.

Cerulus, L., 2020. How Anti-5G Anger Sparked a Wave of Arson Attacks. Adresse : https://www.politico.com/news/2020/04/30/how-anti-5g-anger-sparked-a-wave-of-arson-attacks-across-europe-228050 (consulté en décembre 2022).

CGE – Conférence des grandes écoles, 2022. La gendarmerie nationale développe et valorise les parcours doctoraux. Adresse : https://www.cge.asso.fr/liste-actualites/la-gendarmerie-nationale-developpe-et-valorise-les-parcours-doctoraux/ (consulté en juin 2022).

Chainlink, 2022. What is a DEX (Decentralized Exchange)? Adresse : https://blog.chain.link/dex-decentralized-exchange/#:~:text=A%20decentralized%20exchange%20(DEX)%20is,transfer%20and%20custody%20of%20funds. (consulté en septembre 2022).

Chambre des communes du Canada, 2021. *Projet de loi C-10. Loi modifiant la Loi sur la radiodiffusion et apportant des modifications connexes et corrélatives à d'autres lois*, Ottawa, ON, Chambre des communes du Canada.

Chambre des communes du Canada, 2022. *Projet de loi C-27: Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Ottawa, ON, Chambre des communes du Canada.

Chambre des communes du Canada, s.d. Députés de la 43 législature. Adresse : https://www.noscommunes.ca/Members/fr/search?parliament=43&province=NT (consulté en novembre 2022).

Chambre des représentants des États-Unis, 2018. *Allow States and Victims to Fight Online Sex Trafficking Act of 2017*, Washington, DC, Chambre des représentants des États-Unis.

Chandler, J., 2009. « Privacy vs. National Security: Clarifying the Trade-Off », dans Kerr, I., V. Steeves et C. Lucock(réd.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, NY, Oxford University Press.

Chang, L. Y. C., L. Y. Zhong, et P. N. Grabosky, 2018. « Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime », *Regulation & Governance*, vol. 12, n°1, p. 101-114.

Chertoff, M., 2017. « A public policy perspective of the dark web », *Journal of Cyber Policy* vol. 2, n°1, p. 26-38.

Chesney, B. et D. Citron, 2019. « Deep fakes: A looming challenge for privacy, democracy, and national security », *California Law Review*, vol. 107, p. 1753-1820.

Choi, T., 2019. Canada's Digital Charter Not Strong Enough to Soothe Privacy Concerns on Sidewalk Labs: Critics. Adresse : https://globalnews.ca/news/5337890/canada-digital-charter-sidewalk-labs/ (consulté en mai 2022).

CIGI – Centre for International Governance Innovation, 2021. *Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa*, Waterloo, ON, CIGI.

Citron, D. K., 2009. « Cyber civil rights », *Boston University Law Review*, vol. 89, p. 61-125.

Citron, D. K. et M. A. Franks, 2014. « Criminalizing revenge porn », *Wake Forest Law Review*, vol. 40, p. 345-391.

Citron, D. K. et J. W. Penney, 2019. « When law frees us to speak », *Fordham Law Review*, vol. 87, n°6, p. 2317-2335.

CIVIX Canada, 2022. CTRL-F: Find the Facts. Adresse : https://ctrl-f.ca/en/ (consulté en mai 2022).

CJUE – Cour de justice de l'Union européenne, 2014. *Google Spain SL and Google Inc. v AEPD and Mario Costeja González*, Luxembourg City, Luxembourg, CJUE.

Clark, R., S. Kreps, et A. Rao, 2022. Shifting Crypto Landscape Threatens Crime Investigations and Sanctions. Adresse : https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/ (consulté en juin 2022).

Clearview AI, 2021. Clearview AIs Facial Recognition Platform Achieves Superior Accuracy & Reliability Across All Demographics in NIST Testing. Adresse : https://www.clearview.ai/press-release-nist-facial-recognition-accuracy (consulté en avril 2022).

CMF – Commissariat à la magistrature fédérale Canada, 2022. Nombre de juges de nomination fédérale à compter du 1er mai 2022. Adresse : https://www.fja.gc.ca/appointments-nominations/judges-juges-fra.aspx (consulté en mai 2022).

CMIC – Crypto Market Integrity Coalition, 2022. Public and Unequivocal Pledge. Adresse : https://www.cryptomarketintegrity.com/#The-Pledge (consulté en février 2022).

Cockfield, A. J., 2007. « Protecting the social value of privacy in the context of state investigations using new technologies », *U.B.C. Law Review*, vol. 40, n°1, p. 41-67.

Cohen, I. M., G. Davies, C. Pastia, A. McCormick, Z. Lee, E. Osterberg, … A. Schenk, 2021. *An Examination of The Impact of Court Rulings on Police Investigation Time and Resources*, Abbotsford, BC, University of the Fraser Valley.

Colliver, C., M. Comerford, J. King, A. Krasodomski-Jones, C. Schwieter, et H. Tuck, 2021. *Digital Policy Lab '20 Companion Papers*, Londres, Royaume-Uni, Institute for Strategic Dialogue.

Commission européenne, 2022a. Le paquet législatif sur les services numériques. Adresse : https://digital-strategy.ec.europa.eu/fr/policies/digital-services-act-package (consulté en octobre 2022).

Commission européenne, 2022b. Législation sur les services numériques : La Commission se félicite de l'accord politique sur des règles garantissant un environnement en ligne sûr et responsable. Adresse : https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2545 (consulté en juin 2022).

Commission européenne, s.d. Devons-nous toujours supprimer les données à caractère personnel si une personne le demande? Adresse : https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_fr (consulté en octobre 2022).

Condie, B. et L. Dayton, 2020. Four AI Technologies That Could Transform the Way We Live and Work. Adresse : https://www.nature.com/articles/d41586-020-03413-y (consulté en avril 2022).

Congrès des États-Unis, 2018. *CLOUD Act*, Washington, DC, Congrès des États-Unis.

Congrès des États-Unis, 2022. *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022*, Washington, DC, Congrès des États-Unis.

Cook, J., 2019. Here's What It's Like to See Yourself in a Deepfake Porn Video. Adresse : https://www.huffpost.com/entry/deepfake-porn-heres-what-its-like-to-see-yourself_n_5d0d0faee4b0a3941861fced (consulté en janvier 2022).

Cook, J., 2021. A Powerful New Deepfake Tool Has Digitally Undressed Thousands of Women. Adresse : https://www.huffpost.com/entry/deepfake-tool-nudify-women_n_6112d765e4b005ed49053822 (consulté en janvier 2022).

Corb, A., 2015. « Hate and Hate Crime in Canada », dans Hall, N., A. Corb, P. Giannasi et J. G. D. Grieve(réd.), *The Routledge International Handbook on Hate Crime*, Abingdon, Royaume-Uni, Routledge.

Couvillon, M. A. et V. Ilieva, 2011. « Recommended practices: A review of schoolwide preventative programs and strategies on cyberbullying », *Preventing School Failure*, vol. 55, n°2, p. 96-101.

CPVP – Commissariat à la protection de la vie privée du Canada, 2011. Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée. Adresse : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/ (consulté en avril 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2016a. Comment le Commissariat protège le droit des personnes à la vie privée et en fait la promotion. Adresse : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/mm/ (consulté en août 2021).

CPVP – Commissariat à la protection de la vie privée du Canada, 2016b. Réputation en ligne : Que dit-on à mon sujet? Adresse : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/or_201601/ (consulté en avril 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2017a. Application de la LPRPDE. Adresse : https://priv.gc.ca/biens-assets/compliance-framework/fr/index (consulté en mai 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2017b. Bulletin d'interprétation : Activité commerciale. Adresse : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_03_ca/ (consulté en octobre 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2018. Aperçu des lois sur la protection des renseignements personnels au Canada. Adresse : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/ (consulté en juillet 2021).

CPVP – Commissariat à la protection de la vie privée du Canada, 2019a. *Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019*, Ottawa, ON, OPC.

CPVP – Commissariat à la protection de la vie privée du Canada, 2019b. Survol de la Loi sur la protection des renseignements personnels. Adresse : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels/lprp_survol/ (consulté en juillet 2021).

CPVP – Commissariat à la protection de la vie privée du Canada, 2019c. Survol de la LPRPDE. Adresse : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/lprpde_survol/ (consulté en octobre 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2020a. La vie privée en temps de pandémie. Adresse : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201920/ar_201920/ (consulté en mai 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2020b. Questions et réponses – projet de loi no 64. Adresse : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/qa_20200924/ (consulté en avril 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2021a. *Projeter nos valeurs dans nos lois*, Gatineau, QC, CPVP.

CPVP – Commissariat à la protection de la vie privée du Canada, 2021b. *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte du numérique*, Gatineau, QC, CPVP.

CPVP – Commissariat à la protection de la vie privée du Canada, 2021c. L'utilisation par la GRC (Gendarmerie royale du Canada) de la technologie de reconnaissance faciale de Clearview AI contrevenait à la Loi sur la protection des renseignements personnels, selon une enquête. Adresse : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2021/nr-c_210610/ (consulté en mai 2022).

CPVP – Commissariat à la protection de la vie privée du Canada, 2021d. *Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta*, Ottawa, ON, CPVP.

CPVP – Commissariat à la protection de la vie privée du Canada, 2022. Sensibilisation des enfants à la vie privée. Adresse : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/campagnes-et-activites-de-sensibilisation/sensibilisation-des-enfants-a-la-vie-privee/ (consulté en mai 2022).

Craft, S., S. Ashley, et A. Maksl, 2017. « News media literacy and conspiracy theory endorsement », *Communication and the Public*, vol. 2, n°4, p. 388-401.

Crosby, A., 2021. « Policing right-wing extremism in Canada: Threat frames, ideological motivation, and societal implications », *Surveillance & Society*, vol. 19, n°3, p. 359-363.

Cross, C. et D. Blackshaw, 2015. « Improving the police response to online fraud », *Policing: A Journal of Policy and Practice*, vol. 9, n°2, p. 119-128.

Cross, C., 2016. « 'They're very lonely': Understanding the fraud victimisation of seniors », *International Journal for Crime, Justice and Social Democracy*, vol. 5, n°4, p. 60-74.

Cross, C., K. Richards, et R. Smith, 2016. *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support (Report to the Criminology Research Advisory Council Grant: CRG 29/13-14)*, Canberra, Australie, Australia's Criminology Research Advisory Council.

Cross, C., 2017. « "I've lost some sleep over it": Secondary trauma in the provision of support to older fraud victims », *Canadian Journal of Criminology and Criminal Justice*, vol. 59, n°2, p. 168-197.

Cross, C., T. Holt, A. Powell, et M. Wilson, 2021. « Responding to cybercrime: Results of a comparison between community members and police personnel », *Trends and Issues in Crime and Criminal Justice*, n°635, ti78207.

CRTC – Conseil de la radiodiffusion et des télécommunications Canadiennes, 2022. *Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170*, Ottawa, ON, CRTC.

Crumpler, W. et J. A. Lewis, 2021. *How Does Facial Recognition Work?*, Washington, DC, Center for Strategic & International Studies.

CSC – Cour suprême du Canada, 1990a. *Canada (Commission des droits de la personne) c. Taylor [1990] [1990] 3 RCS 892*, Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 1990b. *R. c. Keegstra [1990] 3 RCS 697*, Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 1995. *Hill c. Église de scientologie de Toronto [1995] 2 RCS 1130*, Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2011. *Bou Malhab c. Diffusion Métromédia CMR inc. [2011] 1 RCS 214*, Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2014a. *Wakeling c. États-Unis d'Amérique, 2014 CSC 72*, vol. [2014] 3 RCS 549. Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2014b. *R. c. Spencer, 2014 CSC 43*, Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2016a. *Banque Royale du Canada c. Trang, 2016 CSC 50*, vol. [2016] 2 RCS 412. Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2016b. *R. c. Jordan, 2016 CSC 27*, vol. 36068. Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2021. *Sherman (Succession) c. Donovan, 2021 CSC 25*, vol. 38695. Ottawa, ON, CSC.

CSC – Cour suprême du Canada, 2022. Registre 40269. Andrei Bykovets c. Sa Majesté le Roi. Adresse : https://www.scc-csc.ca/case-dossier/info/dock-regi-fra.aspx?cas=40269) (consulté en octobre 2022).

CSCB – Cour suprême de la Colombie-Britannique, 2022. *R. v. Coban, 2022 BCSC 1810*, New Westminster, BC, CSCB.

CSJO – Cour supérieure de justice de l'Ontario, 2016. *Doe 464533 v. ND ONSC 541*, Ottawa, ON, CSJO.

CSJO – Cour supérieure de justice de l'Ontario, 2019. *Yenovkian v. Gulian, 2019 ONSC 7279*, Ottawa, ON, CSJO.

CSJO – Cour supérieure de justice de l'Ontario, 2021. *Caplan v. Atas, 2021 ONSC 670*, Ottawa, ON, CSJO.

Culliford, E. et B. Heath, 2021. Facebook Knew About, Failed to Police Abusive Content Globally, Documents Show. Adresse : https://www.reuters.com/technology/facebook-knew-about-failed-police-abusive-content-globally-documents-2021-10-25/ (consulté en avril 2022).

Cumbo-Steinmetz, S., L. Guest, R. Shah, et M. Reynolds, 2020. Ontario recognizes new privacy tort. Adresse : https://www.torys.com/Our%20Latest%20Thinking/Publications//2020/01/ontario-recognizes-new-privacy-tort/ (consulté en juin 2022).

Cusumano, M. A., A. Gawer, et D. B. Yoffie, 2021. Social Media Companies Should Self-Regulate. Now. Adresse : https://hbr.org/2021/01/social-media-companies-should-self-regulate-now (consulté en octobre 2022).

CVMO – Commission des valeurs mobilières de l'Ontario, 2022. Les autorités en valeurs mobilières du Canada s'attendent à ce que les plateformes de négociation de cryptoactifs souscrivent un engagement en attente de leur inscription. Adresse : https://www.osc.ca/fr/nouvelles-evenements/nouvelles/les-autorites-en-valeurs-mobilieres-du-canada-sattendent-ce-que-les-plateformes-de-negociation-de (consulté en septembre 2022).

Cyberaide.ca, 2022a. La Coalition canadienne contre l'exploitation des enfants sur Internet. Adresse : https://cybertip.ca/en/about/ccaice/ (consulté en octobre 2022).

Cyberaide.ca, 2022b. Types de signalements. Adresse : https://cybertip.ca/fr/signalement/types/ (consulté en janvier 2022).

Cyberaide.ca, 2022c. Partenaires. Adresse : https://cybertip.ca/fr/qui-nous-sommes/partenaires/ (consulté en janvier 2022).

Cyberaide.ca, 2022d. Résultats obtenus. Adresse : https://cybertip.ca/fr/qui-nous-sommes/resultats/ (consulté en janvier 2022).

Cyberaide.ca, s.d. L'obligation de signalement. Adresse : https://www.cybertip.ca/fr/qui-nous-sommes/obligation-de-signalement/ (consulté en octobre 2022).

d'Anglejan-Chatillon, A., R. Grewal, É. Lévesque, et C. Vieira, 2021. « The Virtual Currency Regulation Review: Canada », dans Sackheim, M. S. et N. A. Howell(réd.), *The Virtual Currency Regulation Review*, 4th éd., Londres, Royaume-Uni, Law Business Research Ltd.

Daigle, T., 2020. Clearview AI Stops Offering Facial Recognition Software in Canada Amid Privacy Probe. Adresse : https://www.cbc.ca/news/science/clearview-ai-stops-facial-recognition-in-canada-1.5639380 (consulté en avril 2022).

Dan, V., B. Paris, J. Donovan, M. Hameleers, J. Roozenbeek, S. van der Linden, et C. von Sikorski, 2021. « Visual mis- and disinformation, social media, and democracy », *Journalism & Mass Communication Quarterly*, vol. 98, n°3, p. 641-664.

Daswani, Y. et H. Pearson, 2014. Preventing Revenge Porn. Adresse : http://www.keepcalmtalklaw.co.uk/preventing-revenge-porn/ (consulté en août 2021).

Daubs, K., 2022. Scammers Hijacked my Phone Number: There's Nothing I Can Do About Spoofing Attacks. Adresse : https://www.thestar.com/news/gta/2022/01/27/spammers-are-using-my-number-and-theres-nothing-i-can-do-why-spoofed-calls-are-more-than-a-nuisance.html?rf (consulté en février 2022).

Davidson, T., D. Bhattacharya, et I. Weber, 2019. *Racial Bias in Hate Speech and Abusive Language Detection Datasets*, communication présentée dans le cadre du Third Workshop on Abusive Language, Florence, Italy.

Davis, J., 2021. « Old Methods, New Technologies », dans Davis, J.(réd.), *Illicit Money: Financing Terrorism in the Twenty-First Century*, Boulder, CO, Lynne Rienner Publishers.

Dawson, L. L. et A. Amarasingam, 2021. « Homegrown terrorist radicalization: The Toronto 18 in comparative perspective », *Manitoba Law Journal*, vol. 44, n°1, p. 1-33.

De Coninck, D., T. Frissen, K. Matthijs, L. d'Haenens, G. Lits, O. Champagne-Poirier, ... S. Salerno, 2021. « Beliefs in conspiracy theories and misinformation about COVID-19: Comparative perspectives on the role of anxiety, depression and exposure to and trust in information sources », *Frontiers in Psychology*, vol. 12, 646394.

De Hert, P., V. Papakonstantinou, G. Malgieri, L. Beslay, et I. Sanchez, 2018. « The right to data portability in the GDPR: Towards user-centric interoperability of digital services », *Computer Law & Security Review*, vol. 34, n°2, p. 193-203.

Décary-Hétu, D. et L. Giommoni, 2017. « Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous », *Crime, Law and Social Change*, vol. 67, n°1, p. 55-75.

DEDC – Comité mixte spécial sur la déclaration de situation de crise, 2022. *44e Législature, 1re Session, Numéro 007*, Ottawa, ON, Chambre des communes du Canada.

Delwaide, K. et A. Aylwin, 2005. *Leçons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé du Québec.* Ottawa, ON, Commissariat à la protection de la vie privée du Canada.

DeMatteo, M., 2022. Bitcoin Price History: 2009 to 2022. Adresse : https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-price-history/#:~:text=2020%3A%20The%20 Coronavirus%20Pandemic&text=By%20December%202020%2C%20 Bitcoin's%20price,highest%20it%20had%20ever%20been. (consulté en juin 2022).

Dentons, 2021. The Use and Limits of Mutual Legal Assistance Treaties: A Case Study in Canada and the United Kingdom. Adresse : https://www.dentons.com/en/insights/articles/2021/may/27/the-use-and-limits-of-mutual-legal-assistance-treaties-a-case-study-in-canada-and-the-united-kingdom (consulté en mai 2022).

Devlin, K., 2020. Attacks on 5G phone Masts Putting Lives at Risk, No10 Warns Amid Coronavirus Conspiracy Theories. Adresse : https://www.independent.co.uk/news/uk/politics/5g-coronavirus-phone-mast-attack-arson-conspiracy-theory-downing-street-a9450066.html (consulté en décembre 2022).

Dheri, P. et D. Cobey, 2019. Lawful Access and Encryption in Canada: A Policy Framework Proposal. Adresse : http://www.canlii.org/t/sm6c (consulté en février 2022).

DHS – United States Department of Homeland Security, 2021. *National Terrorism Advisory System Bulletin - January 27, 2021*, Washington, DC, DHS.

Di Meco, L., 2019. *#She Persisted: Women, Politics & Power in the New Media World*, Washington, DC, The Wilson Center.

Dias Oliva, T., D. M. Antonialli, et A. Gomes, 2021. « Fighting hate speech, silencing drag queens? Artificial intelligence in content moderation and risks to LGBTQ voices online », *Sexuality & Culture*, vol. 25, n°2, p. 700-732.

Digital Rights Watch, 2021. Explainer: The Online Safety Bill. Adresse : https://digitalrightswatch.org.au/2021/02/11/explainer-the-online-safety-bill/ (consulté en novembre 2021).

Dinha, F., 2021. VPNs May Be Putting Users at Risk. Adresse : https://www.forbes.com/sites/forbestechcouncil/2021/06/08/vpns-may-be-putting-users-at-risk/?sh=29f73cfa6588 (consulté en octobre 2022).

Dizboni, A. et C. Leuprecht, 2020. « Instruments and Arrangements Against Online Terrorism Relating to International Cooperation », dans Vacca, J.(réd.), *Online Terrorist Propaganda, Recruitment, and Radicalization*, Boca Raton, FL, CRC Press.

Dodge, A. et D. C. Spencer, 2018. « Online sexual violence, child pornography, or something else entirely? Police responses to non-consensual intimate image sharing among youth », *Social & Legal Studies*, vol. 27, n°5, p. 636-657.

Dodge, A., 2019. « Nudes are forever: Judicial interpretations of digital technology's impact on "revenge porn" », *Canadian Journal of Law and Society* vol. 34, n°1, p. 121-143.

Dodge, A., D. Spencer, R. Ricciardelli, et D. Ballucci, 2019. « «This isn't your father's police force»: Digital evidence in sexual assault investigations », *Australian & New Zealand Journal of Criminology*, vol. 52, n°4, p. 499-515.

Doffman, Z., 2020. Ashley Madison hack returns to 'haunt' its victims: 32 million users now watch and wait. Adresse : https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/ (consulté en mai 2022).

DOJ – Département de la Justice des États-Unis, 2019a. Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton. Adresse : https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us (consulté en janvier 2022).

DOJ – Département de la Justice des États-Unis, 2019b. Joint US-EU Statement on Electronic Evidence Sharing Negotiations. Adresse : https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations (consulté en janvier 2022).

DOJ – Département de la Justice des États-Unis, 2022a. CLOUD Act Resources. Adresse : https://www.justice.gov/dag/cloudact (consulté en janvier 2022).

DOJ – Département de la Justice des États-Unis, 2022b. United States and Canada Welcome Negotiations of a CLOUD Act Agreement. Adresse : https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement (consulté en mai 2022).

Dolny, T., 2021. « Finding needles in haystacks: Statutory reform recommendations for quasi-criminal insolvencies involving online money laundering », *Annual Review of Insolvency Law*, vol. 19, p. 16.

Donovan, J., 2019. How Hate Groups' Secret Sound System Works. Adresse : https://www.theatlantic.com/ideas/archive/2019/03/extremists-understand-what-tech-platforms-have-built/585136/ (consulté en janvier 2022).

Douek, E., 2020. *The Rise of Content Cartels*, New York, NY, The Knight First Amendment Institute at Columbia University.

DRW – Digital Rights Watch, 2021. *Submission to the Department of Infrastructure, Transport, Regional Development and Communication on the Proposed Online Safety Bill 2020*, Melbourne, Australie, DRW.

Dubois, E. et F. Martin-Bariteau, 2020a. « Citizenship in a Connected Canada », dans Dubois, E. et F. Martin-Bariteau(réd.), *Citizenship in a Connected Canada: A Research and Policy Agenda*, Ottawa, ON, University of Ottawa Press.

Dubois, E. et F. Martin-Bariteau, 2020b. « Next Steps for a Connected Canada », dans Dubois, E. et F. Martin-Bariteau(réd.), *Citizenship in a Connected Canada: A Research and Policy Agenda*, Ottawa, ON, University of Ottawa Press.

Duncanson, S., C. Brinker, K. Twa, et M. O'Neill Sanger, 2021. Federal UNDRIP Bill Becomes Law. Adresse : https://www.osler.com/en/resources/regulations/2021/federal-undrip-bill-becomes-law (consulté en avril 2022).

Dunn, S. et A. Petricone-Westwood, 2018. *More than "Revenge Porn": Civil Remedies for the Non-Consensual Distribution of Intimate Images*, communication présentée dans le cadre du 38th Civil Litigation Conference, Mont-Tremblant, Qc.

Dupont, B., 2016. « La gouvernance polycentrique du cybercrime : Les réseaux fragmentés de la coopération internationale », *Cultures & Conflits*, n°102, p. 95-120.

Dupont, B., 2019. « The Ecology of Cybercrime », dans Leukfeldt, R. et T. J. Holt(réd.), *The Human Factor of Cybercrime*, 1st éd., Abingdon, Royaume-Uni, Routledge.

Dupont, B., 2021. « La police et la prévention de la cybercriminalité », dans Dupont, B., A. Amicelle, R. Boivin, F. Fortin et S. Tanner(réd.), *L'avenir du travail policier*, Montréal, QC, Les Presses de l'Université de Montréal.

Durrani, T., S. Silcoff, et J. O'Kane, 2022. Emergencies Act Won't Stop Protest Funding, Crypto CEO Says. Adresse : https://www.theglobeandmail.com/business/article-emergencies-act-wont-stop-protest-funding-crypto-ceo-says/ (consulté en mars 2022).

Dwoskin, E., J. Whalen, et R. Cabato – 2019. Content Moderators at YouTube, Facebook and Twitter See the Worst of the Web — and Suffer Silently. Adresse : https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/ (consulté en décembre 2022).

Dwoskin, E., W. Oremus, C. Timberg, et N. Tiku, 2021. Racists and Taliban Supporters Have Flocked to Twitter's New Audio Service After Executives Ignored Warnings. Adresse : https://www.washingtonpost.com/technology/2021/12/10/twitter-turmoil-spaces/ (consulté en juin 2022).

Dwoskin, E., N. Tiku, et C. Timberg, 2021. Facebook's Race-Blind Practices Around Hate Speech Came at the Expense of Black Users, New Documents Show. Adresse : https://www.washingtonpost.com/technology/2021/11/21/facebook-algorithm-biased-race/ (consulté en décembre 2022).

Ebner, N. C., D. M. Ellis, T. Lin, H. A. Rocha, H. Yang, S. Dommaraju, ... R. N. Spreng, 2020. « Uncovering susceptibility risk to online deception in aging », *The Journals of Gerontology: Psychological Sciences*, vol. 75, n°3, p. 522-533.

Edmonds, J. et A. Flahault, 2021. « Refugees in Canada during the First Wave of the COVID-19 Pandemic », *International Journal of Environmental Research and Public Health*, vol. 18, n°3, p. 947.

Éducaloi, 2022. Protecting Seniors from Exploitation and Abuse. Adresse : https://educaloi.qc.ca/en/capsules/protecting-seniors-from-exploitation-abuse/ (consulté en janvier 2022).

Edwards, G., L. S. Christensen, S. Rayment-McHugh, et C. Jones, 2021. « Cyber strategies used to combat child sexual abuse material », *Trends & Issues in Crime and Criminal Justice*, n°636, ti78313.

Edwards, L., 2018. « Data Protection: Enter the General Data Protection Regulation », dans Edwards, L.(réd.), *Law, Policy and the Internet*, Londres, Royaume-Uni, Hart Publishing.

EFF – Electronic Frontier Foundation, 2017. *Street-Level Surveillance: Face Recognition*, San Francisco, CA, EFF.

Enders, A. M., J. E. Uscinski, M. I. Seelig, C. A. Klofstad, S. Wuchty, J. R. Funchion, ... J. Stoler, 2021. « The relationship between social media use and beliefs in conspiracy theories and misinformation », *Political Behavior,* vol. Jul 7, p. 1-24.

Equality Now, 2019. The Role of Technology on Facilitating and Addressing Sex Trafficking. Adresse : https://www.equalitynow.org/vienna_may2019 (consulté en août 2021).

eSafety Commissioner, 2021a. *Online Safety Act 2021 Fact Sheet*, Sydney, Australie, Gouvernement de l'Australie.

eSafety Commissioner, 2021b. *Office of the eSafety Commissioner Annual Report 2020-21*, Canberra, Australie, Gouvernement de l'Australie.

eSafety Commissioner, 2022a. New Online Safety Laws Come Into Force. Adresse : https://www.esafety.gov.au/newsroom/media-releases/new-online-safety-laws-come-force (consulté en octobre 2022).

eSafety Commissioner, 2022b. What Is Serious Online Abuse? Adresse : https://www.esafety.gov.au/report/what-is-serious-online-abuse (consulté en janvier 2022).

eSafety Commissioner, s.d.-a. Our Legislative Functions. Adresse : https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions (consulté en juillet 2021).

eSafety Commissioner, s.d.-b. Report to the eSafety Commissioner. Adresse : https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-esafety-commissioner (consulté en janvier 2022).

EDSC – Emploi et Développement social Canada, 2019. *Rapport : Ce que nous avons entendu : Crimes et torts financiers ciblant les aînés*, Ottawa, ON, EDSC.

ETHI – Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 2018. *Vers la protection de la vie privée dès la conception : Examen de la loi sur la protection des renseignements personnels et les documents électroniques*, Ottawa, ON, Chambre des communes du Canada.

ETHI – Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 2021. *Assurer la protection de la vie privée et de la réputation sur les plateformes comme Pornhub*, Ottawa, ON, Chambre des communes du Canada.

ETHI – Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 2022. *Témoignages. Numéro 031. Le lundi,8 août 2022*, Ottawa, ON, Chambre des communes du Canada.

Etteldorf, C., 2021. October Entry into Force for NetzDG Appeal Procedure. Adresse : http://merlin.obs.coe.int/article/9334 (consulté en avril 2022).

Etzioni, A., 2005. « The Limits of Privacy », dans Cohen, A. I. et C. H. Wellman(réd.), *Contemporary Debates in Applied Ethics*, Malden, MA, Blackwell Publishing.

Europol – European Union Agency for Law Enforcement Cooperation, 2020a. *Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic*, La Haye, Pays-Bas, Europol.

Europol – European Union Agency for Law Enforcement Cooperation, 2020b. *Internet Organised Crime Threat Assessment*, La Haye, Pays-Bas, Europol.

Europol – European Union Agency for Law Enforcement Cooperation, 2022. *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, La Haye, Pays-Bas, Europol.

Evans, M., D. Kessler, J. Lennon, et S. Ross, 2019. US CLOUD Act and International Privacy. Adresse : https://www.dataprotectionreport.com/2019/08/u-s-cloud-act-and-international-privacy/ (consulté en octobre 2022).

Facebook – Meta Transparency Center, 2021. Hate Speech. Adresse : https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook/#content-actioned (consulté en novembre 2021).

Facebook, 2020a. Preventing Unwanted Contacts and Scams in Messenger. Adresse : https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/ (consulté en avril 2022).

Facebook, 2020b. Meta: Keeping People Safe and Informed About the Coronavirus. Adresse : https://about.fb.com/news/2020/12/coronavirus/ (consulté en juillet 2021).

Facebook Canada, 2021. *2021 Canadian Election Integrity Initiative: Facebook's Canadian Approach*, Toronto, ON, Facebook Canada.

Facebook Oversight Board, 2019. *Oversight Board Charter,* Menlo Park, CA, Facebook.

Facebook Oversight Board, 2021. *Case Decision 2021-001-FB-FBR*, Menlo Park, CA, Facebook.

Faddoul, M., G. Chaslot, et H. Farid, 2020. « A longitudinal analysis of YouTube's promotion of conspiracy videos », *ArXiv*, 2003.03318.

Faife, C., 2022. Security Experts Say New EU Rules Will Damage WhatsApp Encryption. Adresse : https://www.theverge.com/2022/3/28/23000148/eu-dma-damage-whatsapp-encryption-privacy (consulté en mai 2022).

Faris, R., A. Ashar, U. Gasser, et D. Joo, 2016. *Understanding Harmful Speech Online*, Vol. No. 2016-21. Cambridge, MA, Berkman Klein Center for Internet and Society at Harvard University.

Farrell, H. et A. L. Newman, 2019. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security.* Princeton, NJ, Princeton University Press.

FBI – Federal Bureau of Investigation, 2017. Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay. Adresse : https://www.fbi.gov/news/stories/alphabay-takedown (consulté en août 2021).

FBI – Federal Bureau of Investigation, 2022. Science and Technology Branch. Adresse : https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch (consulté en février 2022).

Feinberg, A., 2017. This Is the Daily Stormer's Playbook. Adresse : https://www.huffpost.com/entry/daily-stormer-nazi-style-guide__n__5a2ece19e4b0ce3b344492f2 (consulté en janvier 2022).

Fenwick, J., 2021. Twitter Says Online Safety Bill Needs More Clarity. Adresse : https://www.bbc.com/news/uk-politics-59010723 (consulté en novembre 2021).

Ferguson, A. G., 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York, NY, New York University Press.

Ferguson, R. I., K. Renaud, S. Wilford, et A. Irons, 2020. « Precept: A framework for ethical digital forensics investigations », *Journal of Intellectual Capital*, vol. 21, n°2, p. 257-290.

FIN – Ministère des Finances Canada, 2022. Le Canada invoque la Loi sur les mesures d'urgence pour limiter le financement des barrages routiers illégaux et rétablir l'ordre public. Adresse : https://www.canada.ca/fr/ministere-finances/nouvelles/2022/02/le-canada-invoque-la-loi-sur-les-mesures-durgencepour-limiter-le-financement-des-barrages-routiers-illegaux-et-retablir-lordre-public.html (consulté en mars 2022).

FINA – Comité permanent des finances, 2018. *Lutte contre le blanchiment d'argent et le financement des activités terroristes : Faire progresser le Canada*, Ottawa, ON, Chambre des communes du Canada.

Finklea, K., 2021. *Law Enforcement and Technology: The "Lawful Access" Debate*, Washington, DC, Congressional Research Service.

Fletcher, E., 2021. Cryptocurrency Buzz Drives Record Investment Scam Losses. Adresse : https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses (consulté en mars 2022).

Forrest, M., 2022. Canada's National Police Force Admits Use of Spyware to Hack Phones. Adresse : https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092 (consulté en octobre 2022).

Frankenfield, J., 2021. Virtual Currency. Adresse : https://www.investopedia.com/terms/v/virtual-currency.asp (consulté en mars 2022).

Frankenfield, J., 2022a. Digital Currency. Adresse : https://www.investopedia.com/terms/d/digital-currency.asp (consulté en août 2022).

Frankenfield, J., 2022b. Cryptocurrency Explained With Pros and Cons for Investment. Adresse : https://www.investopedia.com/terms/c/cryptocurrency.asp (consulté en août 2022).

Franks, M. A., 2018. « Fearless speech », *First Amendment Law Review*, vol. 17, p. 294-342.

Fraser, D., 2022. Most Key Participants in Ottawa Convoy Protest Not Yet Charged. Adresse : https://www.cbc.ca/news/canada/ottawa/convoy-protest-police-ottawa-freedom-trucks-occupation-1.6401510 (consulté en avril 2022).

Freeman Law, 2022. What is a Tumbler, and is Cryptocurrency Tumbling Safe? Adresse : https://freemanlaw.com/what-is-a-tumbler-and-is-cryptocurrency-tumbling-safe/ (consulté en juin 2022).

Frenkel, S. (2021). The Storming of Capitol Hill Was Organized on Social Media. Retrieved décembre 2022, from https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html.

Fry, L. W. et L. J. Berkes, 1983. « The paramilitary police model: An organizational misfit », *Human Organization*, vol. 42, n°3, p. 225-234.

FTC – Federal Trade Commission, 2022. *Social Media a Gold Mine for Scammers in 2021*, Washington, DC, FTC.

Funk, A., 2021. Q&A: Social Media Regulation and the Perils of Section 230 Reform. Adresse : https://freedomhouse.org/article/qa-social-media-regulation-and-perils-section-230-reform (consulté en avril 2022).

Furnell, S., D. Emm, et M. Papadaki, 2015. « The challenge of measuring cyber-dependent crimes », *Computer Fraud & Security*, vol. 2015, n°10, p. 5-12.

Gailey, A. et R. Haar, 2022. The Future of Cryptocurrency: 8 Experts Share Predictions for the Second Half of 2022. Adresse : https://time.com/nextadvisor/investing/cryptocurrency/future-of-cryptocurrency/ (consulté en novembre 2022).

Gallagher, A., J. Davey, et M. Hart, 2020. *The Genesis of a Conspiracy Theory: Key Trends in QAnon Activity Since 2017*, Londres, Royaume-Uni, Institute for Strategic Dialogue.

Gallagher, C., 2021. HSE Confirms Data of 520 Patients Published Online. Adresse : https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136 (consulté en juillet 2022).

Garry, A., S. Walther, R. Rukaya, et A. Mohammed, 2021. « QAnon conspiracy theory: Examining its evolution and mechanisms of radicalization », *Journal for Deradicalization*, vol. 26, p. 152-216.

Gaudette, T., R. Scrivens, et V. Venkatesh, 2020. « The role of the Internet in facilitating violent extremism: Insights from former right-wing extremists », *Terrorism and Political Violence*, p. 1-18.

GC – Gouvernement du Canada, 1982. *Charte canadienne des droits et libertés*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 1985. *Code criminel L.R.C., 1985, ch. C-46*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2000a. *Loi sur la protection des renseignements personnels et les documents électroniques*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2000b. *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2010. *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2011a. *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2011b. *Règlement sur la déclaration de la pornographie juvénile sur Internet*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2014. *Projet de loi C-13: Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2018a. *Loi sur la modernisation des élections*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2018b. Déclaration du président : rencontre des ministres de la Sécurité. Adresse : https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-04-22-security_ministers-ministres_securite.aspx?lang=fra (consulté en mai 2022).

GC – Gouvernement du Canada, 2019a. Traités sur les droits de la personne. Adresse : https://www.canada.ca/fr/patrimoine-canadien/services/systeme-canada-nations-unies/traites.html (consulté en septembre 2022).

GC – Gouvernement du Canada, 2019b. Règlement modifiant certains règlements pris en vertu de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes (2019) : DORS/2019-240. Adresse : https://www.gazette.gc.ca/rp-pr/p2/2019/2019-07-10/html/sor-dors240-fra.html (consulté en août 2022).

GC – Gouvernement du Canada, 2019c. Comprendre la Loi canadienne anti-pourriel. Adresse : https://fightspam-combattrelepourriel.ised-isde.canada.ca/site/loi-canadienne-anti-pourriel/fr/comprendre-loi-canadienne-anti-pourriel/comprendre-loi-canadienne-anti-pourriel-sub/comprendre-loi-canadienne-anti-pourriel (consulté en octobre 2022).

GC – Gouvernement du Canada, 2019d. *Loi sur l'entraide juridique en matière criminelle*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2020a. Guide sur la Charte canadienne des droits et libertés. Adresse : https://www.canada.ca/fr/patrimoine-canadien/services/comment-droits-proteges/guide-charte-canadienne-droits-libertes.html (consulté en janvier 2022).

GC – Gouvernement du Canada, 2020b. *Règlement sur le recyclage des produits de la criminalité et le financement des activités terroristes DORS/2002-184*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2020c. Fiche de renseignements : Loi de 2020 sur la mise en œuvre de la Charte du numérique. Adresse : https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/charte-canadienne-numerique/renforcer-protection-vie-privee-dans-lere-numerique/fiche-renseignements-loi-2020-mise-oeuvre-charte-numerique (consulté en août 2021).

GC – Gouvernement du Canada, 2020d. *Accord Canada–États-Unis–Mexique (ACEUM) - Chapitre 19 - Commerce numérique*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2021a. Modernisation de la Loi sur la protection des renseignements personnels du Canada. Adresse : https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/modern.html (consulté en février 2022).

GC – Gouvernement du Canada, 2021b. Définitions juridiques de la négligence et des mauvais traitements envers les aînés. Adresse : https://www.justice.gc.ca/fra/pr-rp/jp-cj/vf-fv/aines-elder/def/p211.html (consulté en janvier 2022).

GC – Gouvernement du Canada, 2021c. À quel moment vérifier l›identité des personnes et des entités – Entreprises de services monétaires et entreprises de services monétaires étrangères. Adresse : https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/client/msb-fra (consulté en février 2022).

GC – Gouvernement du Canada, 2021d. Monnaie numérique. Adresse : https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/paiment/monnaie-numerique.html (consulté en septembre 2022).

GC – Gouvernement du Canada, 2021e. Collaboration et développement des compétences : renforcer le régime anti-blanchiment d'argent au Canada. Adresse : https://www.canada.ca/fr/securite-publique-canada/nouvelles/2021/12/collaboration-et-developpement-des-competences-renforcer-le-regime-anti-blanchiment-dargent-au-canada.html (consulté en juin 2022).

GC – Gouvernement du Canada, 2021f. *La Loi canadienne anti-pourriel (LCAP) – Rapport de mesure du rendement 2019-2020*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2021g. Guide de discussion. Adresse : https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne/guide-discussion.html (consulté en août 2021).

GC – Gouvernement du Canada, 2021h. *Projet de loi C-36, Loi modifiant le Code criminel, la Loi canadienne sur les droits de la personne et apportant des modifications connexes à une autre loi (propagande haineuse, crimes haineux et discours haineux)*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2021i. Document technique. Adresse : https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne/document-travail-technique.html (consulté en août 2021).

GC – Gouvernement du Canada, 2022a. Allocution de la vice-première ministre et ministre des Finances concernant la Loi sur les mesures d'urgence. Adresse : https://www.canada.ca/fr/ministere-finances/nouvelles/2022/02/allocution-de-la-vice-premiere-ministre-et-ministre-des-finances-concernant-la-loi-sur-les-mesures-durgence.html (consulté en mars 2022).

GC – Gouvernement du Canada, 2022b. *2022 Budget: Un plan pour faire croître notre économie et rendre la vie plus abordable*, Ottawa, ON, GC.

GC – Gouvernement du Canada, 2022c. Une enquête du CRTC cible des fournisseurs et l'administrateur d'un marché du Web invisible. Adresse : https://www.canada.ca/fr/radiodiffusion-telecommunications/nouvelles/2022/01/une-enquete-du-crtc-cible-des-fournisseurs-et-ladministrateur-dun-marche-du-web-invisible.html (consulté en mai 2022).

GC – Gouvernement du Canada, 2022d. Ce que nous avons entendu : Approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne. Adresse : https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne/ce-que-nous-avons-entendu.html (consulté en mai 2022).

GC – Gouvernement du Canada, 2022e. Résumé de la septième séance : lien avec l'application de la loi. Adresse : https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne/resume-septieme-seance.html (consulté en octobre 2022).

GC – Gouvernement du Canada, 2022f. Le gouvernement du Canada annonce la création d'un groupe consultatif d'experts sur la sécurité en ligne. Adresse : https://www.canada.ca/fr/patrimoine-canadien/nouvelles/2022/03/le-gouvernement-du-canada-annonce-la-creation-dun-groupe-consultatif-dexperts-sur-la-securite-en-ligneo.html (consulté en avril 2022).

Geist, M., 2021a. Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation. Adresse : https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/ (consulté en novembre 2021).

Geist, M., 2021b. « "They Just Seemed Not to Listen to Any of Us" - Cynthia Khoo on the Canadian Government's Online Harms Consultation ». *Law Bytes* (23 août).

Geist, M., 2021c. *Government of Canada Consultation on the Proposed Approach to Address Harmful Content Online*, Ottawa, ON, University of Ottawa, Faculty of Law.

Geist, M., 2022a. Not Ready for Prime Time: Why Bill C-11 Leaves the Door Open to CRTC Regulation of User Generated Content. Adresse : https://www.michaelgeist.ca/2022/02/not-ready-for-prime-time/ (consulté en février 2022).

Geist, M., 2022b. The Groundhog Day Privacy Bill: The Government Waited Months to Bring Back Roughly the Same Privacy Plan?! Adresse : https://www.michaelgeist.ca/2022/06/the-groundhog-day-privacy-bill/ (consulté en octobre 2022).

Ghaffary, S., 2021. Facebook Will Push you to Read Articles Before you Share Them. Adresse : https://www.vox.com/2021/5/10/22429240/facebook-prompt-users-read-articles-before-sharing (consulté en juin 2021).

Ghosh, D., 2021a. Are We Entering a New Era of Social Media Regulation? Adresse : https://hbr.org/2021/01/are-we-entering-a-new-era-of-social-media-regulation (consulté en octobre 2022).

Ghosh, S., 2021. Online Misinformation About the US Election Fell 73% After Trump's Social Media Ban. Adresse : https://www.businessinsider.com/misinformation-fell-73-after-trump-was-banned-across-social-media-2021-1 (consulté en décembre 2022).

GIFCT – Global Internet Forum to Counter Terrorism, 2020. *GIFCT Transparency Report July 2020*, Washington, DC, GIFCT.

Gill, L., T. Israel, et C. Parsons, 2018. *Shining a Light on the Encryption Debate: A Canadian Field Guide*, Toronto, ON, The Citizen Lab and The Canadian Internet Policy & Public Interest Clinic.

Gill, L., 2020. *Legal Aspects of Hate Speech in Canada*, Ottawa, ON, Forum des politiques publiques.

Gilmore, R., 2022. Liberals Say New Online Streaming Bill Won't Hurt Free Speech – But Some Remain Skeptical. Adresse : https://globalnews.ca/news/8592505/online-streaming-bill-c-11-free-speech/ (consulté en février 2022).

Global Commission on Internet Governance, 2016. *One Internet*, Waterloo (ON), Centre for International Governance Innovation, Chatham House, The Royal Institute of International Affairs.

Goldfinger, D., 2019. OPP Opens Centre for Cyber Operations. Adresse : https://globalnews.ca/news/5970566/opp-cyber-operations-centre/ (consulté en février 2022).

Goodison, S. E., R. C. Davis, et B. A. Jackson, 2015. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, Santa Monica, CA, RAND Corporation.

Goodwin, J., 2020. Mastercard, Visa and Discover Cut Ties with Pornhub Following Allegations of Child Abuse. Adresse : https://www.cnn.com/2020/12/14/business/mastercard-visa-discover-pornhub/index.html (consulté en octobre 2020).

Google, 2021. Google Transparency Report: YouTube Community Guidelines Enforcement. Adresse : https://transparencyreport.google.com/youtube-policy/removals?hl=en&channels__by__reason=period:2021Q2&lu=comments__removal__reason&comments__removal__reason=period:2021Q2 (consulté en novembre 2021).

Gouv. de l'Australie – Gouvernement de l'Australie, 2010. *Australia's Constitution*, Canberra, Australie, Gouv. de l'Australie.

Gouv. de l'Australie – Gouvernement de l'Australie, 2015. *Enhancing Online Safety Act 2015*, Canberra, Australie, Gouv. de l'Australie.

Gouv. de l'Australie – Gouvernement de l'Australie, 2017. *Enhancing Online Safety for Children Amendment Bill 2017*, Canberra, Australie, Gouv. de l'Australie.

Gouv. de l'Australie – Gouvernement de l'Australie, 2018. *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018*, Canberra, Australie, Gouv. de l'Australie.

Gouv. de l'Australie – Gouvernement de l'Australie, 2019. *Sharing of Abhorrent Violent Material Act Fact Sheet*, Canberra, Australie, Gouv. de l'Australie.

Gouv. de l'Allemagne – Gouvernement de l'Allemagne, 1998. *German Criminal Code*, Berlin, Allemagne, Gouv. de l' Allemagne.

Gouv. du Man. – Gouvernement du Manitoba, 2014. Child Sexual Exploitation. Adresse : https://gov.mb.ca/fs/cfsmanual/1.3.5.html#_Reporting_and_Investigating_1 (consulté en octobre 2022).

Gouv. du Man. – Gouvernement du Manitoba, 2022. *The Child and Family Services Act*, Winnipeg, MB, Gouv. du Man.

Gouv. de la N.-É. – Gouvernement de la Nouvelle-Écosse, 2008b. *Child Pornography Reporting Act*, Halifax, N.-É., Gouv. de la N.-É.

Gouv. de la N.-É. – Gouvernement de la Nouvelle-Écosse, 2022. *Report on the Review of the Intimate Images and Cyber-Protection Act*, Halifax, N.-É., Gouv. de la N.-É.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle Zélande, 1993. *Films, Videos, and Publications Classification Act 1993*, Wellington, Nouvelle-Zélande, Gouv. de la Nouvelle-Zélande.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle Zélande, 2015. *Harmful Digital Communications Act 2015*, Wellington, Nouvelle-Zélande, Gouv. de la Nouvelle-Zélande.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle Zélande, 2021. *Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Act 2021*, Wellington, Nouvelle-Zélande, Gouv. de la Nouvelle-Zélande.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle Zélande, 2022. *Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Act*, Wellington, Nouvelle-Zélande, Gouv. de la Nouvelle-Zélande.

Gouv. du Qc. – Gouvernement du Québec, 1976. *Charte des droits et libertés de la personne*, Québec, Qc, Gouv. du Qc.

Gouv. du Qc. – Gouvernement du Québec, 1982. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, Québec, QC, Gouv. du Qc.

Gouv. du Qc. – Gouvernement du Québec, 1991. *Code civil du Québec*, Québec, Qc, Gouv. du Qc.

Gouv. du Qc. – Gouvernement du Québec, 2021. *Projet de loi nº 64: Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Québec, Qc, Gouv. du Qc.

Gouv. des É.U.– Gouvernement des États-Unis, 2018. *Public Law 115-164 (SESTA/FOSTA)*, Washington, DC, Gouv. des É.U.

Gouv. des É.U.– Gouvernement des États-Unis, s.d.-a. *18 U.S. Code § 373 - Solicitation to Commit a Crime of Violence*, Washington, DC, Gouv. des É.U.

Gouv. des É.U.– Gouvernement des États-Unis, s.d.-b. *18 U.S. Code § 2421A - Promotion or Facilitation of Prostitution and Reckless Disregard of Sex Trafficking*, Washington, DC, Gouv. des É.U.

Gouv. des É.U.– Gouvernement des États-Unis, s.d.-c. *18 U.S. Code Chapter 110 - Sexual Exploitation and Other Abuse of Children*, Washington, DC, Gouv. des É.U.

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni, 2019. *Online Harms White Paper*, Londres, Royaume-Uni, Secretary of State for Digital, Culture, Media & Sport; Secretary of State for the Home Department.

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni,, 2021a. *Online Safety Bill. Explanatory Notes*, Londres, Royaume-Uni, Gouv. du Royaume-Uni.

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni,, 2021b. *Draft Online Safety Bill*, Londres, Royaume-Uni, Gouv. du Royaume-Uni.

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni,, 2021c. National Cyber Strategy 2022 Adresse : https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-force (consulté en janvier 2022).

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni,, 2022. *Online Safety Bill: Factsheet*, Londres, Royaume-Uni, Department for Digital, Culture, Media & Sport.

Grant, I., 2015. « Intimate partner criminal harassment through a lens of responsibilization », *Osgoode Hall Law Journal*, vol. 52, n°2, p. 552-600.

Graves, Z., 2021. The Promise and Perils of Interoperability. Adresse : https://lincolnpolicy.org/2021/the-promise-and-perils-of-interoperability/ (consulté en octobre 2022).

GRC – Gendarmerie royale du Canada, 2014. *Cybercriminalité : survol des incidents et des enjeux au Canada*, Ottawa, ON, GRC.

GRC – Gendarmerie royale du Canada, 2018. La GRC met la population en garde contre un stratagème d'extorsion ciblant les jeunes par l'entremise des réseaux sociaux. Adresse : https://www.rcmp-grc.gc.ca/fr/nouvelles/2018/grc-met-population-garde-stratageme-dextorsion-ciblant-jeunes-lentremise-des-reseaux (consulté en février 2022).

GRC – Gendarmerie royale du Canada, 2019. Stratagèmes de fraude ciblant les nouveaux Canadiens. Adresse : https://www.rcmp-grc.gc.ca/fr/nouvelles/2019/stratagemes-fraude-ciblant-nouveaux-canadiens (consulté en novembre 2021).

GRC – Gendarmerie royale du Canada, 2020a. La GRC branchée. Adresse : https://www.rcmp-grc.gc.ca/fr/grc-branchee (consulté en février 2022).

GRC – Gendarmerie royale du Canada, 2020b. RCMP FSOC Target Dark Web Drug Trafficking Operation. Adresse : https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=2100&languageId=1&contentId=63303 (consulté en août 2021).

GRC – Gendarmerie royale du Canada, 2020c. Groupe national de coordination contre la cybercriminalité. Adresse : https://www.rcmp-grc.gc.ca/fr/groupe-national-coordination-cybercriminalite (consulté en février 2022).

GRC – Gendarmerie royale du Canada, 2021a. Définition de la cybercriminalité. Adresse : https://www.rcmp-grc.gc.ca/fr/definition-cybercriminalite (consulté en octobre 2021).

GRC – Gendarmerie royale du Canada, 2021b. Nouveau système de signalement des incidents de cybercriminalité et de fraude. Adresse : https://www.rcmp-grc.gc.ca/fr/nouveau-systeme-signalement-des-incidents-cybercriminalite-et-fraude (consulté en octobre 2021).

GRC – Gendarmerie royale du Canada, 2021c. Conséquences de l'intimidation et de la cyberintimidation. Adresse : https://www.rcmp-grc.gc.ca/fr/intimidation/consequences-lintimidation-et-cyberintimidation (consulté en juillet 2022).

GRC – Gendarmerie royale du Canada, 2021d. Centre national de coordination en cybercriminalité (CNC3). Adresse : https://www.rcmp-grc.gc.ca/fr/gnc3 (consulté en février 2022).

GRC – Gendarmerie royale du Canada, 2021e. Réponse au rapport du Commissariat à la protection de la vie privée sur l'utilisation de Clearview AI par la GRC. Adresse : https://www.rcmp-grc.gc.ca/fr/nouvelles/2021/reponse-au-rapport-du-commissariat-a-protection-vie-privee-lutilisation-clearview-ai (consulté en juin 2022).

GRC – Gendarmerie royale du Canada, 2022a. Sample Warrant. Adresse : https://www.ourcommons.ca/content/Committee/441/ETHI/WebDoc/WD11922842/11922842/RoyalCanadianMountedPolice-Authorization-e.pdf (consulté en octobre 2022).

GRC – Gendarmerie royale du Canada, 2022b. Entrevue avec un expert en surveillance électronique sur les défis liés à la collecte de preuves. Adresse : https://www.rcmp-grc.gc.ca/fr/gazette/entrevue-expert-surveillance-electronique-defis-lies-a-collecte-preuves?fe=undefined&wbdisable=true (consulté en octobre 2022).

Greene, V. S., 2019. « "Deplorable" satire: Alt-right memes, white genocide tweets, and redpilling normies », *Studies in American Humor*, vol. 5, n°1, p. 31-69.

Grilli, M. D., K. S. McVeigh, Z. M. Hakim, A. A. Wank, S. J. Getz, B. E. Levin, ... R. C. Wilson, 2021. « Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails », *The Journals of Gerontology: Series B*, vol. 76, n°9, p. 1711-1715.

Grygiel, J. et N. Brown, 2019. « Are social media companies motivated to be good corporate citizens? Examination of the connection between corporate social responsibility and social media safety », *Telecommunications Policy*, vol. 43, n°5, p. 445-460.

Guess, A. M., M. Lerner, B. Lyons, J. M. Montgomery, B. Nyhan, J. Reifler, et N. Sircar, 2020. « A digital media literacy intervention increases discernment between mainstream and false news in the United States and India », *Proceedings of the National Academy of Sciences*, vol. 117, n°27, p. 15536-15545.

Guliani, N. S. et N. Shah, 2018. The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them. Adresse : https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them (consulté en avril 2022).

Gullo, K. et K. Rodriguez, 2021. EFF to Council of Europe: Flawed Cross Border Police Surveillance Treaty Needs Fixing - Here Are Our Recommendations to Strengthen Privacy and Data Protections Across the World. Adresse : https://www.eff.org/deeplinks/2021/08/eff-council-europe-flawed-cross-border-police-surveillance-treaty-needs-fixing (consulté en avril 2022).

Gupta, H. et H. Taneja, 2018. WhatsApp has a fake news problem - that can be fixed without breaking encryption. Adresse : https://www.cjr.org/tow_center/whatsapp-doesnt-have-to-break-encryption-to-beat-fake-news.php (consulté en juillet 2021).

Ha-Redeye, O., 2021. Canadian Courts Assume Jurisdiction over Twitter Defamation. Adresse : https://canliiconnects.org/en/commentaries/73241 (consulté en avril 2022).

HabiloMédias, s.d. Propagande haineuse en ligne - Interventions et solutions dans la salle de classe. Adresse : https://habilomedias.ca/litt%C3%A9ratie-num%C3%A9rique-et-%C3%A9ducation-aux-m%C3%A9dias/enjeux-num%C3%A9riques/propagande-haineuse-en-ligne/propagande-haineuse-en-ligne-interventions-et-solutions-dans-la-salle-de-classe (consulté en janvier 2022).

Haggart, B. et N. Tusikov, 2021. How "Free Speech" Kills Internet Regulation Debates: Part Two. Adresse : https://www.cigionline.org/articles/how-free-speech-kills-internet-regulation-debates/ (consulté en octobre 2022).

Hameleers, M., T. E. Powell, T. G. L. A. Van Der Meer, et L. Bos, 2020. « A picture paints a thousand lies? The effects and mechanisms of multimodal disinformation and rebuttals disseminated via social media », *Political Communication*, vol. 37, n°2, p. 281-301.

Hammond, S. et T. Ehret, 2021. *Cryptos On the Rise*, Eagan, MS, Thomson Reuters.

Hango, D., 2016. *La cyberintimidation et le cyberharcèlement chez les utilisateurs d'Internet âgés de 15 à 29 ans au Canada*, Ottawa, ON, Statistique Canada.

Hao, K., 2021. This Is How We Lost Control of Our Faces. Adresse : https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/ (consulté en avril 2022).

Harkin, D., C. Whelan, et L. Chang, 2018. « The challenges facing specialist police cyber-crime units: An empirical analysis », *Police Practice and Research*, vol. 19, n°6, p. 519-536.

Harkin, D. et C. Whelan, 2019. « Exploring the implications of 'low visibility' specialist cyber-crime units », *Australian & New Zealand Journal of Criminology*, vol. 52, n°4, p. 578-594.

Harmon, E., 2017. Sex Trafficking Experts Say SESTA Is the Wrong Solution. Adresse : https://www.eff.org/deeplinks/2017/10/sex-trafficking-experts-say-sesta-wrong-solution (consulté en mars 2022).

Harris, K., 2021. Hundreds Charged Under New Zealand's Harmful Digital Communications Act. Adresse : https://www.nzherald.co.nz/nz/hundreds-charged-under-new-zealands-harmful-digital-communications-act/QA23N4Y4724452UDQKNODTTXXY/ (consulté en novembre 2021).

Harris, T., 2017. How a Handful of Tech Companies Control Billions of Minds Everyday. Adresse : https://www.ted.com/talks/tristan_harris_how_a_handful_of_tech_companies_control_billions_of_minds_every_day?language=en (consulté en août 2021).

Hart, M., J. Davey, E. Maharasingam-Shah, C. O'Connor, et A. Gallagher, 2021. *An Online Environmental Scan of Right-Wing Extremism in Canada*, Londres, Royaume-Uni, Institute for Strategic Dialogue.

Hartzog, W., 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA, Harvard University Press.

Hassan, G., S. Brouillette-Alarie, S. Alava, D. Frau-Meigs, L. Lavoie, A. Fetiu, ... C. Rousseau, 2018. « Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence », *International Journal of Developmental Science*, vol. 12, n°1-2, p. 71-88.

Hatta, M., 2020. « Deep web, dark web, dark net: A taxonomy of "hidden" internet », *Annals of Business Administrative Science*, vol. 19, p. 277-292.

Haugen, F., 2021. *Statement of Frances Haugen*, Sub-Committee on Consumer Protection, Product Safety, and Data Security, United States Senate Committee on Commerce, Science and Transportation, United States Senate.

HCA – High Court of Australia, 2019. *Comcare v Banerji [2019] HCA 23*, Canberra, Australie, HCA.

HCDH – Haut-Commissariat des Nations Unies aux droits de l'homme, 2021. Rapport du Rapporteur spécial sur le droit à la vie privée. Adresse : https://www.ohchr.org/fr/special-procedures/sr-privacy (consulté en janvier 2022).

Heer, T., C. Heath, K. Girling, et E. Bugg, 2021. *Misinformation in Canada: Research and Policy Options*, Ottawa, ON, Evidence for Democracy.

Heldt, A., 2019. « Reading between the lines and the numbers: An analysis of the first NetzDG reports », *Internet Policy Review*, vol. 8, n°2, p. 1-18.

Henry, C. S., K. P. Huynh, et A. Welte, 2018. *Rapport de l'enquête de 2017 sur les modes de paiement*, Ottawa, ON, Banque du Canada.

Henry, N. et A. Powell, 2016. « Sexual violence in the digital age: The scope and limits of criminal law », *Social & Legal Studies*, vol. 25, n°4, p. 397-418.

Hill, K., 2020. The Secretive Company That Might End Privacy as We Know It. Adresse : https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (consulté en octobre 2022).

Hill, K., 2021. Clearview AI's Facial Recognition App Called Illegal in Canada. Adresse : https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html? (consulté en novembre 2022).

Hillier, L., T. Jones, M. Monagle, N. Overton, L. Gahan, J. Blackman, et A. Mitchell, 2010. *Writing Themselves in 3: The Third National Study on the Sexual Health and Wellbeing of Same Sex Attracted and Gender Questioning Young People*, vol. 3. Melbourne, Australie, Australian Research Centre in Sex, Health and Society, La Trobe University.

Hitchcock, A., R. Holmes, et E. Sundorph, 2017. *Bobbies on the Net: A Police Workforce for the Digital Age*, Londres, Royaume-Uni, Reform.

HMIC – Her Majesty's Inspectorate of Constabulary, 2015. *Real Lives, Real Crime*, Londres, Royaume-Uni, HMIC.

Holt, T. J., G. W. Burruss, et A. M. Bossler, 2019. « An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents », *Policing and Society*, vol. 29, n°8, p. 906-921.

Horta Ribeiro, M., S. Jhaver, S. Zannettou, J. Blackburn, G. Stringhini, E. De Cristofaro, et R. West, 2021. « Do platform migrations compromise content moderation? Evidence from r/the_donald and r/incels », *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, n°CSCW2, p. 316.

Horwitz, J. et J. Scheck, 2021. « Facebook Increasingly Suppresses Political Movements It Deems Dangerous ». *The Wall Street Journal* (22 octobre).

Hours, F., 2022. Clap de fin pour les élèves de la toute première e-promotion de l'école de gendarmerie de Chaumont. Adresse : https://www.gendinfo.fr/actualites/2022/clap-de-fin-pour-les-eleves-de-la-toute-premiere-e-promotion-de-l-ecole-de-gendarmerie-de-chaumont (consulté en juin 2022).

HRW – Human Rights Watch, 2018. Germany: Flawed Social Media Law. Adresse : https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law (consulté en juillet 2021).

Huey, L., J. Nhan, et R. Broll, 2013. « 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime », *Criminology & Criminal Justice*, vol. 13, n°1, p. 81-97.

Huey, L. et L. Ferguson, 2022. *Another Digital Divide: Cybersecurity in Indigenous Communities*, London, ON, Western University.

Hunt, A., 2020. Why Our Online Harm Legislation Isn't Working. Adresse : https://adls.org.nz/Story?Action=View&Story_id=225 (consulté en novembre 2021).

Hutchinson, J., A. Amarasingam, R. Scrivens, et B. Ballsun-Stanton, 2021. « Mobilizing extremism online: Comparing Australian and Canadian right-wing extremist groups on Facebook », *Behavioral Sciences of Terrorism and Political Aggression*, 1903064.

Ibrahim, D., 2021. *La traite des personnes au Canada, 2019*, Ottawa, ON, Le Centre canadien de la statistique juridique a publilé.

ICO – Information Commissioner's Office, 2022. *Enforcement Notice*, Wilmslow, Royaume-Uni, ICO.

Igo, S., 2018. *The Known Citizen: A History of Privacy in Modern America*. Cambridge, MA, Harvard University Press.

Ingram, D., 2021. A Tracking Device Made by Apple is Showing up in Suspected Crimes. Adresse : https://www.nbcnews.com/news/apple-airtag-showing-up-crimes-rcna9416 (consulté en mars 2022).

INHOPE – Association of Internet Hotline Providers, 2020. *Annual Report 2020*, Amsterdam, Netherlands, INHOPE Association.

INTERPOL – Organisation internationale de police criminelle, 2021. *National Cybercrime Strategy Guidebook*, Lyon, France, INTERPOL.

Ipsos et NPR, 2020. *Public Poll Findings and Methodology: More Than 1 in 3 Americans Believe a 'Deep State' is Working to Undermine Trump*, Washington, DC, Ipsos et NPR.

Ipsos, 2021. *Online Harm in Journalism*, Toronto, ON, Ipsos.

IRCC – Immigration, Réfugiés et Citoyenneté Canada, 2021a. Fraude visant les nouveaux arrivants. Adresse : https://www.canada.ca/fr/immigration-refugies-citoyennete/services/proteger-fraude/nouveaux-arrivants.html (consulté en novembre 2021).

IRCC – Immigration, Réfugiés et Citoyenneté Canada, 2021b. J'ai reçu des menaces d'une personne qui dit être du service d'immigration. Est-ce une escroquerie? Adresse : https://www.cic.gc.ca/francais/centre-aide/reponse.asp?qnum=1218&top=31 (consulté en février 2022).

ISDE – Innovation, Sciences et Développement économique Canada, 2019. *La Charte numérique du Canada en action : un plan par des Canadiens, pour les Canadiens*, Ottawa, ON, ISDE.

ITV News, 2020. Thousands of Digital Devices Awaiting Analysis by Police Investigators. Adresse : https://www.itv.com/news/2020-04-22/thousands-of-digital-devices-awaiting-analysis-by-police-investigators (consulté en mai 2022).

IWF – Internet Watch Foundation, 2020. The Annual Report 2020: 2020 Trends and Data. Adresse : https://annualreport2020.iwf.org.uk/trends (consulté en août 2021).

Jankowicz, N., J. Hunchak, A. Pavliuc, C. Davies, S. Pierson, et Z. Kaufmann, 2021. *Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online*, Washington, DC, Wilson Center, Science and Technology Innovation Program.

Jeney, P., 2015. *Combatting Child Sexual Abuse Online*, Bruxelles, Belgique, Parlement européen.

Jolley, D., K. M. Douglas, A. C. Leite, et T. Schrader, 2019. « Belief in conspiracy theories and intentions to engage in everyday crime », *British Journal of Social Psychology*, vol. 58, n°3, p. 534-549.

Jolley, D., R. Meleady, et K. M. Douglas, 2020. « Exposure to intergroup conspiracy theories promotes prejudice which spreads across groups », *British Journal of Psychology*, vol. 111, n°1, p. 17-35.

Jolley, D. et J. L. Paterson, 2020. « Pylons ablaze: Examining the role of 5G COVID-19 conspiracy beliefs and support for violence », *British Journal of Social Psychology*, vol. 59, n°3, p. 628-640.

Jones-Jang, S. M., T. Mortensen, et J. Liu, 2021. « Does media literacy help identification of fake news? Information literacy helps, but other literacies don't », *American Behavioral Scientist*, vol. 65, n°2, p. 371-388.

Jones, M. L. et M. E. Kaminski, 2021. « An American's guide to the GDPR », *Denver Law Review*, vol. 98, n°1, p. 93-128.

Judson, E., 2022. *The Online Safety Bill: Demos Position Paper*, Londres, Royaume-Uni, Demos.

JUS – Ministère de la Justice Canada, 2010. Mauvais traitements envers les aînés – Fraude financière commise par des étrangers. Adresse : https://www.justice.gc.ca/fra/pr-rp/jp-cj/vf-fv/ainfr-eldfr/ainfr-eldfr.html (consulté en janvier 2022).

JUS – Ministère de la Justice Canada, 2012. *Harcèlement criminel : guide à l'intention des policiers et des procureurs de la Couronne*, Ottawa, ON, JUS.

JUS – Ministère de la Justice Canada, 2019. Document d'information législatif : loi modifiant le Code criminel, la Loi sur le système de justice pénale pour les adolescents et d'autres lois et apportant des modifications corrélatives à certaines lois, tel qu'elle a été édictée (projet de loi C-75 lors de la 42e législature). Adresse : https://www.justice.gc.ca/fra/pr-rp/sjc-csj/sjp-jsp/c75/p2.html (consulté en mars 2022).

JUS – Ministère de la Justice Canada, 2020. *Évaluation de l'Initiative sur les pouvoirs d'enquête au 21e siècle*, Ottawa, ON, JUS.

JUS – Ministère de la Justice Canada, 2021. Qu'est-ce que la traite des personnes? Adresse : https://www.justice.gc.ca/fra/jp-cj/tp/quoi-what.html (consulté en mars 2022).

JUST – Comité permanent de la justice et des droits de la personne, 2019. *Agir pour mettre fin à la haine en ligne : rapport du comité permanent de la justice et des droits de la personne*, Ottawa, ON, Chambre des communes du Canada.

Justiz Online, 2022. Gericht entscheidet über Eilanträge von Google und Meta: Netzwerkdurchsetzungsgesetz verstößt teilweise gegen Unionsrecht. Adresse : https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/05_01032022/index.php (consulté en avril 2022).

Kalpakis, G., T. Tsikrika, N. Cunningham, C. Iliou, S. Vrochidis, J. Middleton, et I. Kompatsiaris, 2016. « OSINT and the Dark Web », dans Akhgar, B., P. S. Bayerl et F. Sampson(réd.), *Open Source Intelligence Investigation: From Strategy to Implementation*, Cham, Switzerland, Springer International Publishing Ag.

Kan, M., 2020. Pornhub Purges 10 Million Videos After Losing Credit Card Support. Adresse : https://www.pcmag.com/news/pornhub-purges-10-million-videos-after-losing-credit-card-support (consulté en octobre 2020).

Kanstrén, T., 2021. Mapping Ring Signatures and Stealth Addresses in Monero. Adresse : https://medium.com/coinmonks/mapping-ring-signatures-and-stealth-addresses-in-monero-a5543a434684 (consulté en août 2022).

Karadeglija, A., 2022. Regulating Cryptocurrency Under Emergencies Act Not as Clear as Freeland Suggests. Adresse : https://nationalpost.com/news/politics/regulating-cryptocurrency-under-emergencies-act-not-as-clear-as-freeland-suggests (consulté en mars 2022).

Karasavva, V. et A. Noorbhai, 2021. « The real threat of deepfake pornography: A review of Canadian policy », *Cyberpsychology, Behavior, and Social Networking*, vol. 24, n°3, p. 203-209.

Keatinge, T., D. Carlisle, et F. Keen, 2018. *Virtual Currencies and Terrorist Financing: Assessing The Risks and Evaluating Responses*, Bruxelles, Belgique, Parlement européen.

Keller, D., 2021. Empirical Evidence of Over-Removal by Internet Companies Under Intermediary Liability Laws: An Updated List. Adresse : http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws (consulté en novembre 2021).

Kendrick, L., 2012. *Speech, Intent and the Chilling Effect*, Charlottesville, VA, University of Virginia School of Law.

Kenyon, M., 2021. Bill C-11 Explained. Adresse : https://citizenlab.ca/2021/04/bill-c-11-explained/ (consulté en juillet 2021).

Kerr, I. et J. McGill, 2007. « Emanations, snoop dogs and reasonable expectations of privacy », *Criminal Law Quarterly*, vol. 52, n°3, p. 392-431.

Kerr, I. et J. Barrigar, 2012. « Privacy, Identity and Anonymity », dans Ball, K., K. Haggerty et D. Lyon(réd.), *International Handbook of Surveillance Studies*, Londres, Royaume-Uni, Routledge.

Ketchum, A., 2020. *Report on the State of Resources Provided to Support Scholars Against Harassment, Trolling, and Doxxing While Doing Public Media Work and How University Media Relations Offices/Newsrooms Can Provide Better Support*, Montréal, QC, Medium.

Kethineni, S. et Y. Cao, 2020. « The rise in popularity of cryptocurrency and associated criminal activity », *International Criminal Justice Review*, vol. 30, n°3, p. 325-344.

Khan, I., 2021. *Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, vol. A/HRC/47/25. Geneva, Switzerland, United Nations Human Rights Council.

Khan, R. et T. Ali Hakami, 2022. « Cryptocurrency: Usability perspective versus volatility threat », *Journal of Money and Business*, vol. 2, n°1, p. 16-28.

Khoo, B., R. C. W. Phan, et C. H. Lim, 2021. « Deepfake attribution: On the source identification of artificially generated images », *WIREs Data Mining and Knowledge Discovery*.

Khoo, C., K. Robertson, et R. Deibert, 2019. *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*, Toronto, ON, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto.

Khoo, C., 2021. *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence*, Toronto, ON, Women's Legal Education & Action Fund.

Kiedrowski, J., R.-F. Melchers, R. Ruddell, et M. Petrunik, 2015. *The Civilianization of Police in Canada*, Ottawa, ON, Public Safety Canada.

Klonick, K., 2018. « The New Governors: The People, Rules, and Processes Governing Online Speech », *Harvard Law Review*, vol. 131, p. 1598-1670.

Klonick, K., 2020. « The Facebook Oversight Board: Creating an independent institution to adjudicate online free expression », *The Yale Law Journal*, vol. 129, n°2418, p. 2418-2499.

Klosowski, T., 2020. Facial Recognition Is Everywhere. Here's What We Can Do About It. Adresse : https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ (consulté en avril 2022).

Koczerginski, M., 2021. Cyber Justice: Ontario Court Recognizes New Tort of Internet Harassment. Adresse : https://mcmillan.ca/insights/cyber-justice-ontario-court-recognizes-new-tort-of-internet-harassment/ (consulté en juin 2022).

Koepke, L., E. Weil, U. Janardan, T. Dada, et Y. Harlan, 2020. *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Washington, DC, Upturn.

Kong, J., J. Ip, C. Huang, et K. Lin, 2021. *One Year of Racist Attacks: Anti-Asian Racism Across Canada One Year into the COVID-19 Pandemic*, Toronto, ON, Chinese Canadian National Council Toronto Chapter.

Kostelac, C. A., 2008. *The Changing Face of Police Organizations: Trends in Civilianization.* Tempe (AZ), Arizona State University.

Kowalski, M., 2002. *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Ottawa, ON, Statistique Canada.

Krasodomski-Jones, A., 2021. *The Liberal Democratic Internet - Five Models for a Digital Future*, Londres, Royaume-Uni, Digital Policy Lab, Institute for Strategic Dialogue.

Kratz, M., 2018. 514-BILLETS Pays $100,000 - CASL Still Being Enforced After Critical Reviews. Adresse : http://www.slaw.ca/2018/05/25/514-billets-pays-100000-casl-still-being-enforced-after-critical-reviews/ (consulté en mai 2022).

Kratz, M., 2019. Digital Intermediaries Can Be Responsible for Unknown CASL Violations - New CRTC Guidance on S.9 Anti-Spam Compliance. Adresse : http://www.slaw.ca/2019/01/24/digital-intermediaries-can-be-responsible-for-unknown-casl-violations-new-crtc-guidance-on-s-9-anti-spam-compliance/ (consulté en mai 2022).

Kratz, M., 2020. CRTC Enforces CASL in Case of Malware Distribution. Adresse : http://www.slaw.ca/2020/01/03/crtc-enforces-casl-in-case-of-malware-distribution/ (consulté en mai 2022).

Krishnamurthy, V., A. L. Lenner, M. Sali, V. van Houden, S. Crothers, J. Nguyen, … B. Horton, 2020. *CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States*, Ottawa, ON, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa (CIPPIC).

Krishnamurthy, V., D. Schmidt, et A. Lehr, 2021. « Cybersecurity and Human Rights: Understanding the Connection », dans Andrew, J. et F. Bernard(réd.), *Human Rights Responsibilities in the Digital Age: States, Companies and Individuals*, 1 éd., Oxford, Royaume-Uni, Hart Publishing.

Kristof, N. – 2020. The Children of Pornhub. Adresse : https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html (consulté en décembre 2022).

Kukutai, T. et J. Taylor, 2016. *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australie, ANU Press.

Laidlaw, E. et H. Young, 2017. *Internet Intermediary Liability in Defamation: Proposals for Statutory Reform*, Toronto, ON, Law Commission of Ontario.

Laidlaw, E., 2019. *Mapping Current and Emerging Models of Intermediary Liability*, Calgary, AB, University of Calgary.

Laidlaw, E. et H. Young, 2020. « Creating a revenge porn tort for Canada », *Supreme Court Law Review*, vol. 2020, p. 147-187.

Laidlaw, E., 2021a. The Future of the Tort of Privacy: Is Alberta's Lag Its Opportunity to Lead? Adresse : https://nationalmagazine.ca/en-ca/articles/law/opinion/2021/the-future-of-the-tort-of-privacy (consulté en mars 2022).

Laidlaw, E., 2021b. *Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows*, Calgary, AB, Global Affairs Canada.

Lam, S., O. Ferlatte, et T. Salway, 2019. « Cyberbullying and health: A preliminary investigation of the experiences of Canadian gay and bisexual adult men », *Journal of Gay & Lesbian Social Services*, vol. 31, n°3, p. 332-357.

Landau, S., 2011. *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. Cambridge, MA, MIT Press.

Landau, S., 2017. *Listening In: Cybersecurity in an Insecure Age*. Grand Rapids, MI, Yale University Press.

Lane, A. M., 2022. Crypto Theft is on the Rise. Here's How the Crimes Are Committed, and How You Can Protect Yourself. Adresse : https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027 (consulté en mars 2022).

Lang, H., 2022. Major Cryptocurrency Firms Launch New Coalition to Promote Market Integrity. Adresse : https://www.theglobeandmail.com/business/international-business/article-major-cryptocurrency-firms-launch-new-coalition-to-promote-market/ (consulté en février 2022).

Langlois, S. et F. Sauvageau, 2021. La désinformation et les médias sociaux, le couple qui inquiète. Adresse : https://www.ledevoir.com/opinion/idees/594300/la-desinformation-et-les-medias-sociaux-le-couple-qui-inquiete (consulté en décembre 2022).

LCJC – Comité permanent affaires juridiques et constitutionnelles, 2017. *Justice différée, justice refusée : l'urgence de réduire les longs délais dans le système judiciaire au canada.* Ottawa, ON, Sénat du Canada.

Le Pennec, G., I. Fiedler, et L. Ante, 2021. « Wash trading at cryptocurrency exchanges », *Finance Research Letters*, vol. 43, 101982.

Leinwand, J., 2018. Expanding Our Policies on Voter Suppression. Adresse : https://about.fb.com/news/2018/10/voter-suppression-policies/ (consulté en août 2022).

Lemstra, M., M. Rogers, L. Redgate, M. Garner, et J. Moraros, 2011. « Prevalence, risk indicators and outcomes of bullying among on-reserve First Nations youth », *Canadian Journal of Public Health*, vol. 102, n°6, p. 462-466.

Leonardi, P. M. et E. Vaast, 2016. « Social Media and Their Affordances for Organizing: A Review and Agenda for Research », *Academy of Management Annals*, vol. 11, n°1, p. 150-188.

Leslie, D., 2020. *Understanding Bias in Facial Recognition Technologies*, Londres, Royaume-Uni, The Alan Turing Institute.

Leukfeldt, R., S. Veenstra, et W. Stol, 2013. « High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands », *International Journal of Cyber Criminology*, vol. 7, n°1, p. 1-17.

Leuprecht, C., 2019. *Where to Draw the Blue Line: How Civilians and Contractors Can Let Police Do The Policing*, Ottawa, ON, Macdonald-Laurier Institute.

Levi, M., 2017. « Assessing the trends, scale and nature of economic cybercrimes: Overview and issues », *Crime, Law and Social Change*, vol. 67, p. 3-20.

Library of Congress, 2021. Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech. Adresse : https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/ (consulté en novembre 2021).

Liebhardt, J., 2008. Australia Rallies to "Stop the Clean Feed." Adresse : https://globalvoices.org/2008/12/11/australia-rallies-to-stop-the-clean-feed/ (consulté en février 2022).

LII – Legal Information Institute, s.d. Tort. Adresse : https://www.law.cornell.edu/wex/tort#:~:text=A%20tort%20is%20an%20act%20or%20omission%20that,in%20fact%20that%20an%20individual%20suffers.%201%20Overview (consulté en mars 2022).

Lin, S., S. Hernandez, et T. Castleman, 2022. Accused Pelosi Attacker David DePape Spread QAnon, Other Far-Right, Bigoted Conspiracies. Adresse : https://www.latimes.com/california/story/2022-10-28/pelosi-attack-suspect-david-depape-shared-conspiracy-theories (consulté en novembre 2022).

Ling, J. et J. Pearson, 2016. Exclusive: Canadian Police Obtained Blackberry's Global Decryption Key. Adresse : https://www.vice.com/en/article/kz9kaa/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how (consulté en octobre 2022).

Ling, J., 2022. Was it Really about Vaccine Mandates — or Something Darker? The Inside Story of the Convoy Protests. Adresse : https://www.thestar.com/news/canada/2022/03/19/was-it-really-about-vaccine-mandates-or-something-darker-the-inside-story-of-the-convoy-protests.html (consulté en décembre 2022).

Little, S., 2022. Exclusive: Mountie Who Worked Amanda Todd Case Speaks for First Time. Adresse : https://globalnews.ca/news/9050914/amanda-todd-officer-speaks/ (consulté en novembre 2022).

Llanso, E. J., 2020. « No amount of "AI" in content moderation will solve filtering's prior-restraint problem », *Big Data & Society*, vol. 7, n°1, 2053951720920686.

Louie, D. W., 2017. « Social media and the sexual exploitation of Indigenous girls », *Girlhood Studies*, vol. 10, n°2, p. 97-113.

Loveluck, B., 2020. « The many shades of digital vigilantism: A typology of online self-justice », *Global Crime*, vol. 21, n°3-4, p. 213-241.

Lucock, C. et K. Black, 2009. « Anonymity and Law in Canada », dans Kerr, I., V. Steeves et C. Lucock(réd.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, NY, Oxford University Press.

Lukings, M. et A. H. Lashkari, 2022a. *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance*. Cham, Switzerland, Springer Cham.

Lukings, M. et A. H. Lashkari, 2022b. *Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective*. Cham, Switzerland, Springer Nature.

Lyons, K., 2021. Clearview's Facial Recognition Tech is Illegal Mass Surveillance, Canada Privacy Commissioners Say. Adresse : https://www.theverge.com/2021/2/4/22266055/clearview-facial-recognition-illegal-mass-surveillance-canada-privacy (consulté en novembre 2022).

Mac, R. et K. Hill, 2021. Are Apple AirTags Being Used to Track People and Steal Cars? Adresse : https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html (consulté en décembre 2022).

Macaulay, K., 2021. How Is Canada Addressing Non-Consensual Intimate Image Distribution? Adresse : https://www.mcgill.ca/definetheline/article/how-canada-addressing-non-consensual-intimate-image-distribution (consulté en novembre 2022).

MacCarthy, M., 2022. What U.S. Policymakers Can Learn from the U.K.'s Online Safety Bill. Adresse : https://www.brookings.edu/blog/techtank/2022/05/19/what-u-s-policymakers-can-learn-from-the-u-k-s-online-safety-bill/ (consulté en juin 2022).

MacDonald, M., 2021. The Double Exploitation of Deepfake Porn. Adresse : https://thewalrus.ca/the-double-exploitation-of-deepfake-porn/ (consulté en janvier 2022).

Macguire, E., 2020. Anti-Asian Hate Continues to Spread Online Amid COVID-19 Pandemic. Adresse : https://www.aljazeera.com/news/2020/4/5/anti-asian-hate-continues-to-spread-online-amid-covid-19-pandemic (consulté en décembre 2022).

Mackey, J., 2012. « Privacy and the Canadian media: Developing the new tort of "intrusion upon seclusion" with Charter values », *Western Journal of Legal Studies*, vol. 2, n°1, p. 3.

Madiega, T., 2020. *Reform of the EU Liability Regime for Online Intermediaries*, Bruxelles, Belgique, European Parliamentary Research Service.

Madiega, T., 2021. *Digital Services Act.* Bruxelles, Belgique, European Parliamentary Research Service.

Malone, M., 2021. *Canadian Businesses Need Better Tools to Report Cybercrime*, Ottawa, ON, Institute for Research on Public Policy.

Maras, M.-H. et A. Alexandrou, 2018. « Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos », *The International Journal of Evidence & Proof*, vol. 23, n°3, p. 255-262.

Martin, A., 2021. What is the Online Safety Bill and Why are Some People Worried About it? Adresse : https://news.sky.com/story/what-is-the-online-safety-bill-and-why-are-some-people-worried-about-it-12437427 (consulté en novembre 2021).

Marwick, A. et R. Lewis, 2017. *Media Manipulation and Disinformation Online*, New York, NY, Data & Society Research Institute.

Maschmeyer, L., R. J. Deibert, et J. R. Lindsay, 2021. « A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society », *Journal of Information Technology & Politics*, vol. 18, n°1, p. 1-20.

Masoodi, M. J. et A. Rand, 2021. *Why Canada Must Defend Encryption.*, Toronto, ON, Ryerson University's Cybersecure Policy Exchange.

Matthes, J., D. Schmuck, et C. von Sikorski, 2021. « In the eye of the beholder: A case for the visual hostile media phenomenon », *Communication Research*, 00936502211018596.

Mazowita, B. et M. Vézina, 2014. *Les cybercrimes déclarés par la police au Canada, 2012, 2012*, Ottawa, ON, Statistique Canada.

McClelland, C., 2021. Data Brokers Are Tracking You — and Selling the Info. Adresse : https://financialpost.com/technology/data-brokers-are-tracking-you-and-selling-the-info (consulté en mai 2022).

McFarlane, G., 2021. How Facebook (Meta), Twitter, Social Media Make Money From You. Adresse : https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx#toc-the-bottom-line (consulté en octobre 2022).

McGuire, M. R., 2017. « Technology Crime and Technology Control: Contexts and History », dans McGuire, M. R. et T. J. Holt(réd.), *The Routledge Handbook of Technology, Crime and Justice*, Abingdon, Royaume-Uni, Routledge.

Mckim, N., 2021. Greens Reject Online Safety Bill. Adresse : https://greensmps.org.au/articles/greens-reject-online-safety-bill (consulté en novembre 2021).

McMillan, 2018. What Can The Law Do About 'Deepfake'? Adresse : https://mcmillan.ca/insights/what-can-the-law-do-about-deepfake/ (consulté en avril 2022).

McMillan, 2021. Adoption du project de loi no 64 : modernisation du régime de protection de la vie privée. Adresse : https://mcmillan.ca/fr/perspectives/adoption-du-projet-de-loi-no-64-modernisation-du-regime-de-protection-de-la-vie-privee/ (consulté en avril 2022).

McNamee, M. S., 2021. HSE cyber-attack: Irish health service still recovering months after hack. Adresse : https://www.bbc.com/news/world-europe-58413448 (consulté en mai 2022).

Mcquigge, M., 2018. Airbnb Rentals Being Used for Alleged Human Trafficking: Toronto Police. Adresse : https://www.theglobeandmail.com/news/toronto/airbnb-rentals-being-used-for-alleged-human-trafficking-toronto-police/article38066008/ (consulté en mai 2022).

Merrill, J. B. et W. Oremus, 2021. Five Points for Anger, One for a 'Like': How Facebook's Formula Fostered Rage and Misinformation. Adresse : https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/ (consulté en January 2022).

Mertl, S., 2013. No one rushing to emulate Nova Scotia's cyberbullying law. Adresse : https://ca.news.yahoo.com/blogs/dailybrew/no-one-rushing-emulate-nova-scotia-cyberbullying-law-224843238.html (consulté en novembre 2021).

Meyer, C., 2021. Canada looks at Australia's experience regulating social media. Adresse : https://www.thestar.com/news/canada/2021/02/02/canada-looks-at-australias-experience-regulating-social-media.html (consulté en juillet 2021).

Ministère de l'Intérieur (France), 2019. Un insigne militaire pour valoriser les gendarmes docteurs. Adresse : https://www.gendarmerie.interieur.gouv.fr/pjgn/actus/un-insigne-militaire-pour-valoriser-les-gendarmes-docteurs (consulté en juin 2022).

Misitzis, L., 2021. « There. I Fixed It. ». *This American Life* (2 juillet).

Mizrahi, S., 2018. « Ontario's new invasion of privacy torts: Do they offer monetary redress for violations suffered via the Internet of Things? », *Western Journal of Legal Studies*, vol. 8, n°1, p. 3.

Molla, R., 2021. Right-Wing Extremists' Favorite New Platform Is So Dangerous. Adresse : https://www.vox.com/recode/22238755/telegram-messaging-social-media-extremists (consulté en septembre 2022).

Monk, B., J. Mitchell, R. Frank, et G. Davies, 2018. « Uncovering Tor: An examination of the network structure », *Security and Communication Networks*, 4231326.

Moonshot CVE, 2021. *Redirect Method Canada: Final Report*, Londres, Royaume-Uni, Moonshot CVE.

Moreau, G., 2021a. *Statistiques sur les crimes déclarés par la police au Canada, 2020*, Ottawa, ON, Statistique Canada.

Moreau, G., 2021b. *Les crimes haineux déclarés par la police au Canada, 2019*, Ottawa, ON, Statistique Canada.

Mortensen, M. et C. Neumayer, 2021. « The playful politics of memes », *Information, Communication & Society*, vol. 24, n°16, p. 2367-2377.

Müller, K. et C. Schwarz, 2020a. « From hashtag to hate crime: Twitter and anti-minority sentiment », *SSRN*, 3149103

Müller, K. et C. Schwarz, 2020b. « Fanning the flames of hate: Social media and hate crime », *SSRN*, 3082972.

Mullins, S. J., 2013. « "Global Jihad": The Canadian experience », *Terrorism and Political Violence*, vol. 25, n°5, p. 734-776.

Musharbash, Y., 2021. *The Globalization of Far-Right Extremism: An Investigative Report*, West Point, NY, Combating Terrorism Center.

NACCC – North American Cyber Classification Compendium, 2021. *Cyber Classification Compendium*, Ottawa (ON), Cybercrime Support Network, Canadian Association of Chiefs of Police, E-Crimes Cyber Council.

NACCC – North American Cyber Classification Compendium, 2021b. North American Cyber Classification Compendium Infographic, Ottawa (ON), Cybercrime Support Network, Canadian Association of Chiefs of Police, E-Crimes Cyber Council.

Nakashima, E. et B. Gellman, 2015. As Encryption Spreads, U.S. Grapples With Clash Between Privacy, Security. Adresse : https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?postshare=531428699926574 (consulté en avril 2014).

NCMEC – National Center for Missing & Exploited Children, 2021. COVID-19 and Missing & Exploited Children. Adresse : https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children (consulté en août 2021).

NeedHelpNow.ca, 2022. Removing Pictures/Videos. Adresse : https://www.needhelpnow.ca/app/en/removing_pictures (consulté en janvier 2022).

Negreiro, M., 2020. *Curbing the Surge in Online Child Abuse: The Dual Role of Digital Technology in Fighting and Facilitating its Proliferation*, Bruxelles, Belgique, Parlement européen.

Nesbitt, M. et T. Hansen, 2021. « Enforcing Canadian Security Laws through Criminal Prosecutions during a Pandemic: Lessons from Canada's COVID-19 Experience », dans West, L., T. Juneau et A. Amarasingam(réd.), *Stress Tested: The COVID-19 Pandemic and Canadian National Security*, Calgary, AB, University of Calgary Press.

Netsafe, 2021. What is the HDCA? Adresse : https://www.netsafe.org.nz/what-is-the-hdca/ (consulté en juillet 2021).

New Zealand Police, 2021. *New Zealand Police Expert Panel on Emergent Technologies. Terms of Reference*, Wellington, New Zealand, New Zealand Police.

New Zealand Police, 2022. Advisory Panel on Emergent Technologies. Adresse : https://www.police.govt.nz/about-us/programmes-and-initiatives/police-use-emergent-technologies/advisory-panel-emergent (consulté en avril 2022).

Newton, C., 2019. The Trauma Floor: The Secret Lives of Facebook Moderators in America. Adresse : https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona (consulté en avril 2022).

Newton, C., 2020. Everything You Need to Know About Section 230. Adresse : https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation (consulté en novembre 2021).

NLCA – Cour d'appel de Terre-Neuve-et-Labrador, 2019. Référence : Décision relative à l'article 487.02 du Code criminel, 2019 NLCA 6. Adresse : https://www.canlii.org/fr/nl/nlca/doc/2019/2019nlca6/2019nlca6.html (consulté en novembre 2022).

Nisker, J., 2006. « PIPEDA: A constitutional analysis », *Canadian Bar Review*, vol. 85, n°2, p. 317-343.

Nissenbaum, H., 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, Stanford Law Books.

Nobles, M., B. W. Reyns, K. Fox, et B. S. Fisher, 2014. « Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample », *Justice Quarterly*, vol. 31, n°6, p. 986-1014.

Nogrady, B., 2021. « Scientists under attack », *Nature*, vol. 598, p. 250-253.

Nordal, S., 2013. *Privacy as a Social Concept*, Calgary, AB, University of Calgary.

Northcott, P., 2021. Civilian Investigators Coming to RCMP. Adresse : https://www.rcmp-grc.gc.ca/en/gazette/civilian-investigators-coming-rcmp?h= (consulté en février 2022).

Northcott, P., 2022. RCMP Training Officers on Cryptocurrency. Adresse : https://www.rcmp-grc.gc.ca/en/gazette/rcmp-training-officers-cryptocurrency (consulté en septembre 2022).

Norton Rose Fulbright, 2012. Rights of Action for Breach of Privacy in Canada. Adresse : https://www.mondaq.com/canada/corporate/175580/rights-of-action-for-breach-of-privacy-in-canada (consulté en avril 2022).

Nosák, D., 2021. The DSA Introduces Important Transparency Obligations for Digital Services, but Key Questions Remain. Adresse : https://cdt.org/insights/the-dsa-introduces-important-transparency-obligations-for-digital-services-but-key-questions-remain/ (consulté en juin 2022).

Novak, M., J. Grier, et D. Gonzales, 2019. New Approaches to Digital Evidence and Acquisition and Analysis. Adresse : https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis (consulté en mai 2022).

NS DOJ – Nova Scotia Department of Justice, 2008. Mandatory Reporting of Child Pornography. Adresse : https://novascotia.ca/news/release/?id=20081030006 (consulté en octobre 2022).

NSF – National Science Foundation, 2019. Facial Recognition Software Has a Gender Problem. Adresse : https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=299486 (consulté en avril 2022).

NSPCC – National Society for the Prevention of Cruelty to Children, 2020. Instagram Most Recorded Platform Used in Child Grooming Crimes During Lockdown. Adresse : https://www.nspcc.org.uk/about-us/news-opinion/2020/instagram-grooming-crimes-children-lockdown (consulté en septembre 2022).

NSSC – Supreme Court of Nova Scotia, 2015. *Crouch v. Snell, 2015 NSSC 340*, Halifax (NS), NSSC.

NSWP – Global Network of Sex Work Projects, 2018. *The Impact of Anti-Trafficking Legislation and Initiatives on Sex Workers*, Edinburgh, Royaume-Uni, NSWP.

NU – Organisation des Nations unies, 1948. *Déclaration universelle des droits de l'homme*, vol. 999. Paris, France, Assemblée générale des Nations Unies.

NU – Organisation des Nations unies, 1966. *Pacte international relatif aux droits civils et politiques*, Paris, France, Assemblée générale des Nations Unies.

NU – Organisation des Nations unies, 2007. *Déclaration des Nations Unies sur les droits des peuples autochtones*, Paris, France, Assemblée générale des Nations Unies.

O'Connor, C., 2021. *Gaming and Extremism: The Extreme Right on Twitch*, Londres, Royaume-Uni, Institute for Strategic Dialogue.

O'Regan, M., 2019. Airbnb Must Face the Facts: Human Trafficking and Modern Slavery Happen in Rented Accommodation. Adresse : https://news.airbnb.com/expanding-our-efforts-to-combat-human-trafficking/ (consulté en mai 2022).

OAIC – Office of the Australian Information Commissioner, 2021. Clearview AI Breached Australians' Privacy. Adresse : https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy (consulté en octobre 2022).

OCDE – Organisation de coopération et de développement économiques, 2020a. *Combattre la désinformation sur le COVID-19 sur les plateformes en ligne*, Paris, France, OCDE.

OCDE – Organisation de coopération et de développement économiques, 2020b. *Approches actuelles des 50 principaux services mondiaux de partage de contenus en ligne face aux contenus terroristes et extrémistes violents*, Paris, France, OCDE.

OCDE – Organisation de coopération et de développement économiques, 2021. *Data Portability, Interoperability and Digital Platform Competition*, Paris, France, OCDE.

Ofcom, 2020. Ofcom to Regulate Harmful Content Online. Adresse : https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/ofcom-to-regulate-harmful-content-online#:~:text=The%20Government%20has%20decided%20to,benefits%20of%20being%20online%20safely. (consulté en juillet 2021).

Ohm, P., 2010. « Broken promises of privacy: Responding to the surprising failure of anonymization », *UCLA Law Review*, vol. 57, p. 1701-1777.

Olser, s.d. Conformité à la Loi canadienne anti-pourriel : plus que du pourriel. Adresse : https://www.osler.com/fr/ressources/cap-sur/conformite-a-la-loi-canadienne-anti-pourriel-plus-que-du-pourriel (consulté en mai 2022).

Olteanu, A., C. Castillo, J. Boy, et K. R. Varshney, 2018. *The Effect of Extremist Violence on Hateful Speech Online*, communication présentée dans le cadre du Proceedings of the Twelfth International AAAI Conference on Web and Social Media, Palo Alto, CA.

ONCA – La Cour d'appel de l'Ontario, 2012. *Jones v. Tsige 2012 ONCA 32*, Toronto, ON, ONCA.

ONCJ – Cour de justice de l'Ontario, 2021. *R. v. Hurren, 2021 ONCJ 148*, Ottawa, ON, ONCJ.

OnlyFans, 2020. *Privacy Policy*. Londres, Royaume-Uni, OnlyFans.

ONUDC – Office des Nations unies contre la drogue et le crime, 2015. *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, Vienna, Austria, Organisation des Nations unies.

Osipovich, A., 2021. Upstart Peer-to-Peer Crypto Exchanges Take Aim at Coinbase. Adresse : https://www.wsj.com/articles/upstart-peer-to-peer-crypto-exchanges-take-aim-at-coinbase-11621848601 (consulté en avril 2022).

OSSNR – Office de surveillance des activités en matière de sécurité nationale et de renseignement, 2019a. *La relation entre le scrs et la grc vue sous l'angle d'une enquête en cours (examen de l'ossnr no 2019-04)*, Ottawa, ON, OSSNR.

Owen, T., P. Loewen, D. Ruths, A. Bridgman, R. Gorwa, S. MacLellan, … O. Zhilin, 2019. *Digital Democracy Project: Research Memo #3 - Polarization and its Discontents*, Ottawa, ON, Forum des politiques publiques.

Paikin, S., 2020. « How Extremists Are Exploiting COVID-19 ». *The Agenda* (13 mai).

Palmer, D., 2021. Businesses Don't Know How to Manage VPN Security Properly - and Cyber Criminals Are Taking Advantage. Adresse : https://www.zdnet.com/article/many-organisations-dont-know-how-to-manage-vpn-security-properly-and-cyber-criminals-are-taking-advantage/ (consulté en octobre 2022).

Paris, B. et J. Donovan, 2019. *Deepfakes and Cheap Fakes*, New York, NY, Data & Society.

Parker, S., 2021. *Le Recueil de cyberclassification nord-américain*, vol. printemps/été 2021. Kanata (ON), Canadian La revue des chefs de police du Canada.

Parlement allemand, 2017. *Act to Improve Enforcement of the Law in Social Networks*, Berlin, Allemagne, Parlement allemand.

Parlement du Royaume-Uni – Parlement du Royaume-Uni, 2022a. *Online Safety Bill*, Londres, Royaume-Uni, Chambre des communes.

Parlement du Royaume-Uni – Parlement du Royaume-Uni, 2022b. *Online Safety Bill [As Amended on Report]*, Londres, Royaume-Uni, Chambre des communes.

Parlement du Royaume-Uni – Parlement du Royaume-Uni, 2022a. *Online Safety Bill*, Londres, Royaume-Uni, Chambre des communes.

Parlement européen, 2022. Législation sur les services numériques: garantir des espaces en ligne plus sûrs. Adresse : https://www.europarl.europa.eu/news/fr/press-room/20220114IPR21017/legislation-sur-les-services-numeriques-garantir-des-espaces-en-ligne-plus-surs (consulté en octobre 2022).

Parsons, C., 2014. Canadian Cyberbullying Legislation Threatens to Further Legitimize Malware Sales. Adresse : https://christopher-parsons.com/canadian-cyberbullying-legislation-threatens-to-further-legitimize-malware-sales/ (consulté en avril 2022).

Parsons, C., 2016. Pleading the Case: How the RCMP Fails to Justify Calls for New Investigatory Powers. Adresse : https://christopher-parsons.com/pleading-the-case-how-the-rcmp-fails-to-justify-calls-for-new-investigatory-powers/ (consulté en février 2022).

Parsons, C. et A. Molnar, 2018. « Government surveillance accountability: The failures of contemporary Canadian interception reports », *Canadian Journal of Law and Technology*, vol. 16, n°1, p. 4.

Parsons, C., 2019. Canada's New and Irresponsible Encryption Policy. Adresse : https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/ (consulté en août 2021).

Parsons, C., 2022. Lawful Access Returns: Online Harms and Warrantless Access to Subscriber and Transmission Data. Adresse : https://christopher-parsons.com/lawful-access-returns-online-harms-and-warrantless-access-to-subscriber-and-transmission-data/ (consulté en avril 2022).

Parsons, P., 2021. Prosecutor Shortage Puts 1,200 Court Cases at Risk, Says Alberta Crown Attorneys' Association. Adresse : https://www.cbc.ca/news/canada/edmonton/alberta-crown-prosecutor-shortage-1.6255359 (consulté en avril 2022).

Patil, S., 2019. *Partnering for Prosperity: India-Canada Collaboration to Curb Digital Black Markets*, Waterloo, ON, Centre for International Governance Innovation and Gateway House.

Pavlounis, D., J. Johnston, J. Brodsky, et P. Brooks, 2022. *The Digital Media Literacy Gap: How to Build Widespread Resilience to False and Misleading Information Using Evidence-Based Classroom Tools*, Toronto, ON, CIVIX Canada.

Pearson, J. et J. Ling, 2016. Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages. Adresse : https://www.vice.com/en/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada (consulté en février 2022).

Pennell, D., M. Campbell, D. Tangen, et A. Knott, 2022. « Should Australia have a law against cyberbullying? Problematising the murky legal environment of cyberbullying from perspectives within schools », *The Australian Educational Researcher*, vol. 49, p. 827-844.

Penney, J., 2017. « Internet surveillance, regulation, and chilling effects online: A comparative case study », *Internet Policy Review*, vol. 6, n°2, 2017.2012.2692.

Penney, J., 2019a. « Chilling effects and transatlantic privacy », *European Law Journal*, vol. 25, p. 122-139.

Penney, J., 2019b. « Privacy and legal automation: The DMCA as a case study », *Stanford Technology Law Review*, vol. 22, n°2, p. 412-486.

Penney, J., 2020. « Online Abuse, Chilling Effects, and Human Rights », dans Dubois, E. et F. Martin-Bariteau(réd.), *Citizenship in a Connected Canada: A Policy and Research Agenda*, Ottawa, ON, University of Ottawa Press.

Penney, J., 2022. « Understanding chilling effects », *Minnesota Law Review*, vol. 106, n°3, p. 1451-1530.

Pennycook, G., A. Bear, E. T. Collins, et D. G. Rand, 2020. « The implied truth effect: Attaching warnings to a subset of fake news headlines increases perceived accuracy of headlines without warnings », *Management Science*, vol. 66, n°11, p. 4944-4957.

Pennycook, G., Z. Epstein, M. Mosleh, A. A. Arechar, D. Eckles, et D. G. Rand, 2021. « Shifting attention to accuracy can reduce misinformation online », *Nature*, vol. 592, n°7855, p. 590-595.

Perrigo, B., 2022. Inside Facebook's African Sweatshop. Adresse : https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/ (consulté en avril 2022).

Perrin, W., L. Woods, et M. Walsh, 2021. Secretary of State's Powers and the Draft Online Safety Bill. Adresse : https://www.carnegieuktrust.org.uk/blog-posts/secretary-of-states-powers-and-the-draft-online-safety-bill/ (consulté en novembre 2021).

Perry, B. et R. Scrivens, 2016. « Uneasy alliances: A look at the right-wing extremist movement in Canada », *Studies in Conflict & Terrorism*, vol. 39, n°9, p. 819-841.

Pew Research Center, 2017. *Online Harassment 2017*, Washington, DC, Pew Research Center.

Pfefferkorn, R., 2020. The EARN IT Act: How to Ban End-to-End Encryption without Actually Banning It. Adresse : https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it (consulté en avril 2022).

Pfefferkorn, R., 2022. « Content-oblivious trust and safety techniques: Results from a survey of online service providers », *Journal of Online Trust and Safety*, vol. 1, n°2, jots.v1i2.14.

Plan International, 2020a. *Free to be Online?: Girls' and Young Women's Experiences of Online Harassment*, Surrey, Royaume-Uni, Plan International.

Plan International, 2020b. Abuse and Harassment Driving Girls Off Facebook, Instagram and Twitter. Adresse : https://plan-international.org/news/2020-10-05-abuse-and-harassment-driving-girls-facebook-instagram-and-twitter (consulté en août 2021).

Police1 BrandFocus Staff, 2018. Analyze and Share Digital Evidence Faster with a Tool Developed by and for Police. Adresse : https://www.police1.com/police-products/investigation/computer-digital-forensics/articles/analyze-and-share-digital-evidence-faster-with-a-tool-developed-by-and-for-police-3Z5uUyAYZ1MQwXWJ/ (consulté en mai 2022).

Pollino, M. A., 2021. « Turning points from victim to survivor: An examination of sexual violence narratives », *Feminist Media Studies*, 14680777.14682021.12006260.

Popham, J., M. McCluskey, M. Ouellet, et O. Gallupe, 2020. « Exploring police-reported cybercrime in Canada: Variation and correlates », *Policing: An International Journal*, vol. 43, n°1, p. 35-48.

Pornhub, 2020. The Latest on Our Commitment to Trust and Safety. Adresse : https://www.pornhub.com/blog/the-latest-on-our-commitment-to-trust-and-safety (consulté en octobre 2020).

Pornhub, 2022. Non-Consensual Content Policy. Adresse : https://help.pornhub.com/hc/en-us/articles/360041719433-Non-Consensual-Content-Policy (consulté en mars 2022).

Porter, J., 2021. Apple Scrubs Controversial CSAM Detection Feature from Webpage But Says Plans Haven't Changed. Adresse : https://www.theverge.com/2021/12/15/22837631/apple-csam-detection-child-safety-feature-webpage-removal-delay (consulté en octobre 2022).

Posetti, J., K. Bontchev, et N. Shabbir, 2022. *The Chilling: Assessing Big Tech's Response to Online Violence Against Women Journalists*, Paris, France, UNESCO.

Posner, R., 2007. *United States vs. Garcia*, Madison, WI, United States Court of Appeals, Seventh Circuit.

Powell, A. et N. Henry, 2018. « Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives », *Policing and Society*, vol. 28, n°3, p. 291-307.

Powell, T. E., H. G. Boomgaarden, K. De Swert, et C. H. de Vreese, 2015. « A clearer picture: The contribution of visuals and text to framing effects », *Journal of Communication*, vol. 65, n°6, p. 997-1017.

PrevNet, 2014. *Cyber Bullying and How it is Affecting Canadian Youth*, Kingston, ON, Queen's University.

Price, M., 2022. Mastercard, Visa Suspend Ties with Ad Arm of Pornhub Owner MindGeek. Adresse : https://www.reuters.com/business/finance/mastercard-visa-suspend-ties-with-ad-arm-pornhub-owner-mindgeek-2022-08-04/ (consulté en octobre 2022).

Prichard, J., R. Wortley, P. A. Watters, C. Spiranovic, C. Hunn, et T. Krone, 2022. « Effects of automated messages on internet users attempting to access 'barely legal' pornography », *Sexual Abuse*, vol. 34, n°1, p. 106-124.

Proctor, J., 2020. The Difficult History of Prosecuting Hate in Canada. Adresse : https://www.cbc.ca/news/canada/british-columbia/racists-attacks-court-hate-crimes-1.5604912 (consulté en juillet 2021).

Projet Arachnid, 2022. *Shield par Projet Arachnid*. Adresse : https://www.projectarachnid.ca/fr/#shield (consulté en février 2022).

Projet Tor, 2022. Users: Relay Users. Adresse : https://metrics.torproject.org/userstats-relay-country.html (consulté en septembre 2022).

Pyrik, J., 2021. « The Financial Transactions and Reports Analysis Center of Canada (FINTRAC) », dans Carvin, S., T. Juneau et C. Forcese(réd.), *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, Toronto, ON, University of Toronto Press.

Qarri, A., 2022. Canada Must Reform Competition and Privacy Policy Together to Protect Consumers. Adresse : https://policyoptions.irpp.org/magazines/february-2022/canada-must-reform-competition-and-privacy-policy-together-to-protect-consumers/ (consulté en juin 2022).

Rakheja, H., 2021. Despite Privacy Fears, Aadhaar-Linked Facial Recognition Used For Covid-19 Vaccines. Adresse : https://inc42.com/buzz/despite-privacy-fears-facial-recognition-used-for-covid-19-vaccines/ (consulté en avril 2022).

Raman-Wilms, M. et B. Curry, 2021. What is Bill C-10 and why are the liberals planning to regulate the Internet? Adresse : https://www.theglobeandmail.com/politics/article-what-is-bill-c-10-and-why-are-the-liberals-planning-to-regulate-the/ (consulté en juillet 2021).

Rao, S., A. K. Verma, et T. Bhatia, 2021. « A review on social spam detection: Challenges, open issues, and future directions », *Expert Systems with Applications*, vol. 186, p. 115742.

RCSP – Réseau Canadien du savoir policier, 2021. Cadre de gestion axé sur les compétences pour les compétences numériques des policiers canadiens. Adresse : https://www.cpkn.ca/wp-content/uploads/Complete-French_CBMF_Digital_Competencies_Report_June17_2021.pdf (consulté en janvier 2022).

RCSP – Réseau Canadien du savoir policier, 2022. Catalogue de cours. Adresse : https://www.cpkn.ca/fr/catalogue-de-cours/ / (consulté en février 2022).

Reed, C., 2007. « Taking Sides on Technology Neutrality », *SCRIPT-ed*, vol. 4, n°3, p. 263-284.

Reep-van den Bergh, C. M. et M. Junger, 2018. « Victims of Cybercrime in Europe: A review of victim surveys », *Crime Science*, vol. 7, p. 5.

Reporters Without Borders, 2018. The Network Enforcement Act Apparently Leads to Excessive Blocking of Content. Adresse : https://rsf.org/en/news/network-enforcement-act-apparently-leads-excessive-blocking-content (consulté en novembre 2021).

Reuters, 2022. German Court Rules Against Online Hate-Speech Law. Adresse : https://www.reuters.com/world/europe/german-court-rules-against-online-hate-speech-law-2022-03-01/ (consulté en avril 2022).

Rice, E. S., E. Haynes, P. Royce, et S. C. Thompson, 2016. « Social media and digital technology use among Indigenous young people in Australia: A literature review », *International Journal for Equity in Health*, vol. 15, n°1, p. 81.

Rid, T., 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York, NY, Farrar, Straus and Giroux.

Ridgeway, G., 2018. « Policing in the Era of Big Data », *Annual Review of Criminology*, vol. 1, p. 401-419.

Rigano, C., 2019. « Using artificial intelligence to address criminal justice needs », *NIJ Journal*, vol. 280, n° janvier, p. 1-10.

Roberts, S. T., 2019. *Behind the Screen: Content Moderation in the Shadows of Social Media*. New Haven, CT, Yale University Press.

Robertson, A., 2021. Facebook is Shutting Down Its Face Recognition Tagging Program. Adresse : https://www.theverge.com/2021/11/2/22759613/meta-facebook-face-recognition-automatic-tagging-feature-shutdown (consulté en avril 2022).

Robertson, K., C. Khoo, et Y. Song, 2020. *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*, Toronto, ON, The Citizen Lab.

Robinson, N. et J. Whittaker, 2020. « Playing for Hate? Extremism, terrorism, and videogames », *Studies in Conflict & Terrorism*, 1057610X.1052020.1866740.

Rogers, R., 2020. « Deplatforming: Following extreme internet celebrities to Telegram and alternative social media », *European Journal of Communication*, vol. 35, n°3, p. 213-229.

Rohlfing, S., 2015. « Hate on the Internet », dans Hall, N., A. Corb, P. Giannasi et J. G. D. Grieve(réd.), *The Routledge International Handbook on Hate Crime*, Abingdon, Royaume-Uni, Routledge.

Romano, A., 2018. A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as we Know it. Adresse : https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom (consulté en septembre 2018).

Roose, K., 2021. What Is QAnon, the Viral Pro-Trump Conspiracy Theory? Adresse : https://www.nytimes.com/article/what-is-qanon.html (consulté en décembre 2022).

Rottweiler, B. et P. Gill, 2020. « Conspiracy beliefs and violent extremist intentions: The contingent effects of self-efficacy, self-control and law-related morality », *Terrorism and Political Violence*, vol. 34, n°7, p. 1485-1504.

Saliba, J., 2021. My Technology Can...Speed Up Digital Evidence Processing. Adresse : https://www.policemag.com/613434/my-technology-can-speed-up-digital-evidence-processing (consulté en mai 2022).

Samsung, 2021. Evolving for the Better: SmartThings Ecosystem Gives Galaxy Users Better Control Over Their Connected Devices. Adresse : https://www.samsungmobilepress.com/press-releases/evolving-for-the-better-smartthings-ecosystem-gives-galaxy-users-better-control-over-their-connected-devices?path=%2Fpressreleases%2Fevolving-for--the-better-smartthings-ecosystem-gives-galaxy-users-better-control-over-their-connected-devices (consulté en octobre 2022).

Samsung, s.d. Galaxy SmartTag. Adresse : https://www.samsung.com/ca/mobile-accessories/galaxy-smarttag-black-ei-t5300bbegca/ (consulté en octobre 2022).

Sandle, P., 2022. UK Ditches Ban on 'Legal but Harmful' Online Content in Favour of Free Speech. Adresse : https://www.reuters.com/world/uk/uk-ditches-ban-legal-harmful-online-content-favour-free-speech-2022-11-28/ (consulté en décembre 2022).

Sap, M., D. Card, S. Gabriel, Y. Choi, et N. A. Smith, 2019. *The Risk of Racial Bias in Hate Speech Detection*, communication présentée dans le cadre du the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy.

Scassa, T., 2018. Enforcement Powers Key to PIPEDA Reform. Adresse : https://policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/ (consulté en octobre 2022).

Scassa, T., 2020. « A Human Rights-Based Approach to Data Protection in Canada », dans Dubois, E. et F. Martin-Bariteau(réd.), *Citizenship in a Connected Canada: A Research and Policy Agenda*, Ottawa, ON, University of Ottawa Press.

Scassa, T., 2021. Data Mobility (Portability) in Canada's Bill C-11. Adresse : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=338:data-mobility-portability-in-canadas-bill-c-11&Itemid=80 (consulté en novembre 2021).

Scassa, T., 2022a. Anonymization and De-Identification in Bill C-27. Adresse : http://teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80 (consulté en octobre 2022).

Scassa, T., 2022b. Bill C-27's Take on Consent: A Mixed Review. Adresse : http://teresascassa.ca/index.php?option=com_k2&view=item&id=355:bill-c-27%E2%80%99s-take-on-consent-a-mixed-review&Itemid=80 (consulté en octobre 2022).

Scassa, T., 2022c. Data Sharing for Public Good: Does Bill C-27 Reflect Lessons Learned from Past Public Outcry? Adresse : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=357:data-sharing-for-public-good-does-bill-c-27-reflect-lessons-learned-from-past-public-outcry?&Itemid=80&tmpl=component&print=1 (consulté en octobre 2022).

Scheck, J., N. Purnell, et J. Horwitz, 2021. « Facebook Employees Flag Drug Cartels and Human Traffickers: The Company's Response is Weak, Documents Show ». *The Wall Street Journal* (16 septembre).

Schiebinger, L., I. Klinge, I. Sánchez de Madariaga, H. Y. Paik, M. Schraudner, et M. Stefanick, 2021. *Facial Recognition: Analyzing Gender and Intersectionality in Machine Learning*. Adresse : https://genderedinnovations.stanford.edu/methods/gender.html (consulté en septembre 2022)..

Schöpfel, J., 2019. « Grey Literature and Professional Knowledge Making », dans Börjesson, L. et I. Huvila(réd.), *Research Outside The Academy: Professional Knowledge-Making in the Digital Age*, Cham, Switzerland, Springer International Publishing.

Schwartz, B., M. Adeler, M. Myschyshyn, et R. Walichnowski, 2021. « Ethical and legal obligations of lawyers to consider cybersecurity », *Asper Review of International Business and Trade Law*, vol. 21, p. 25-57.

Scott-Railton, J., E. Campo, B. Marczak, B. A. Razzak, S. Anstis, G. Böcü, ... R. Deibert, 2022. CatalanGate : Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. Adresse : https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ (consulté en mai 2022).

Scrivens, R., G. Davies, et R. Frank, 2020. « Measuring the evolution of radical right-wing posting behaviors online », *Deviant Behavior*, vol. 41, n°2, p. 216-232.

SCRS – Service canadien du renseignement de sécurité, 2018. Qui dit quoi? *Défis sécuritaires découlant de la désinformation aujourd'hui*, Ottawa, ON, SCRS.

SCRS – Service canadien du renseignement de sécurité, 2021a. *Rapport public du SCRS 2020*, Ottawa, ON, SCRS.

SCRS – Service canadien du renseignement de sécurité, 2021b. *Menaces d'ingérence étrangère visant les processus démocratiques du Canada*, Ottawa, ON, SCRS.

SCRS – Service canadien du renseignement de sécurité, 2022. *Protéger la sécurité nationale en partenariat avec tous les Canadiens*, Ottawa, ON, SCRS.

SECU – Comité permanent de la sécurité publique et nationale, 2021. *Racisme systémique au sein des services policiers au Canada*, Ottawa, ON, Chambre des communes du Canada.

SECU – Comité permanent de la sécurité publique et nationale, 2022a. *La montée de l'extrémisme violent à caractère idéologique au Canada - 44e Législature, 1re Session*, Ottawa, ON, Chambre des communes du Canada.

SECU – Comité permanent de la sécurité publique et nationale, 2022b. *44e Législature, 1re Session, Numéro 012*, Ottawa, ON, Chambre des communes du Canada.

Seering, J., T. Wang, J. Yoon, et G. Kaufman, 2019. « Moderator engagement and community development in the age of algorithms », *New Media & Society*, vol. 21, n°7, p. 1417-1443.

Selim, G., 2019. *Mass Violence, Extremism, and Digital Responsibility: Testimony of George Selim Senior Vice President for National Programs ADL (Anti-Defamation League) at a Hearing Before the Senate Committee on Commerce, Science and Transportation*, Washington, DC, The United States Senate.

Shahani, A., 2014. Smartphones are Used to Stalk, Control Domestic Abuse Victims. Adresse : https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims (consulté en 2022).

Shao, C., G. L. Ciampaglia, O. Varol, K.-C. Yang, A. Flammini, et F. Menczer, 2018. « The spread of low-credibility content by social bots », *Nature Communications*, vol. 9, 4787.

Sheils, C., 2021. Enter The Deep and Dark Web If You Dare (And Get Ready For A Surprise). Adresse : https://digital.com/online-privacy/deep-dark-web/ (consulté en février 2022).

Shin, J., L. Jian, K. Driscoll, et F. Bar, 2018. « The diffusion of misinformation on social media: Temporal pattern, message, and source », *Computers in Human Behavior*, vol. 83, p. 278-287.

Short, E., A. Brown, M. Pitchford, et J. Barnes, 2017. « Revenge porn: Findings from the harassment and revenge porn (HARP) survey - preliminary results », *Annual Review of Cybertherapy and Telemedicine*, vol. 15, p. 161-166.

Shute, R., E. Vernon, M. Verastegui-Sanchez, M. Dix, et M. Planty, 2021. *Landscape Study of Digital Tools to Identify, Capture, and Analyze Digital Evidence in Technology-Facilitated Abuse Cases*, Research Triangle Park, NC, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Siminovic, D., 2017. *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on Violence Against Women, its Causes and Consequences*, Toronto, ON, Citizen Lab, Munk School of Global Affairs, University of Toronto.

Simonite, T., 2018. Photo Algorithms ID White Men Fine - Black Women, Not So Much. Adresse : https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/ (consulté en avril 2022).

Simple Rate, 2021. Credit Card Fraud Statistics in Canada 2021. Adresse : https://www.simplerate.ca/credit-card-fraud-statistics-canada/ (consulté en juillet 2022).

Singh, A., 2015. Hacking Team Leak Highlights Citizen Lab Research. Adresse : https://citizenlab.ca/2015/08/hacking-team-leak-highlights-citizen-lab-research/ (consulté en avril 2022).

Sly, S. et T. Wheeler, 2022. An Education-Based Approach to Curbing CSAM Production. Adresse : https://www.brookings.edu/techstream/an-education-based-approach-to-curbing-csam-production/ (consulté en avril 2022).

Smith, T., 2021a. Cryptocurrency Regulations Around the World. Adresse : https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122 (consulté en février 2022).

Smith, D., 2021b. Here's What Died on the Order Paper. Adresse : https://www.nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2021/here-s-what-died-on-the-order-paper (consulté en mai 2022).

Sobowale, J., 2021. A New Era for Crypto. Adresse : https://www.nationalmagazine.ca/en-ca/articles/legal-market/regulatory/2021/a-new-era-for-crypto (consulté en février 2022).

Solomon, H., 2022. Canadian Internet Providers Must Block Bad Botnets, Says Regulator. Adresse : https://www.itworldcanada.com/article/canadian-internet-providers-must-block-bad-botnets-says-regulator/490160 (consulté en octobre 2022).

Solove, D. J., 2002. « Conceptualizing privacy », *California Law Review*, vol. 90, p. 1087-1156.

Solove, D. J., 2006. « A taxonomy of privacy », *University of Pennsylvania Law Review*, vol. 154, n°3, p. 477-560.

Solove, D. J., 2008. *Understanding Privacy*. Cambridge, MA, Harvard University Press.

Solove, D. J., 2015. « The Meaning and Value of Privacy », dans Roessler, B. et D. Mokrosinska(réd.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge, Royaume-Uni, Cambridge University Press.

SP – Sécurité publique Canada, 2017a. Réunion ministérielle des cinq pays 2017 : Communiqué conjoint. Adresse : https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/index-fr.aspx (consulté en octobre 2022).

SP – Sécurité publique Canada, 2017b. *Rapport public de 2017 sur la Menace terroriste pour le Canada*, Ottawa, ON, SP.

SP – Sécurité publique Canada, 2019a. Le gouvernement du Canada annonce des initiatives pour contrer l'extrémisme violent et le contenu terroriste en ligne. Adresse : https://www.canada.ca/fr/securite-publique-canada/nouvelles/2019/06/le-gouvernement-du-canada-annonce-des-initiatives-pour-contrer-lextremisme-violent-etlecontenu-terroriste-en-ligne.html (consulté en novembre 2021).

SP – Sécurité publique Canada, 2019b. *Rapport public de 2018 sur la Menace terroriste pour le Canada*, Ottawa, ON, SP.

SP – Sécurité publique Canada, 2020. Déclaration internationale : chiffrement de bout en bout et sécurité publique. Adresse : https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2020-jnt-sttmnt-ncrptn-pblc-sfty/index-fr.aspx (consulté en février 2022).

SP – Sécurité publique Canada, 2021a. La cyberintimidation peut avoir de sérieuses conséquences . Adresse : https://www.canada.ca/fr/securite-publique-canada/campagnes/cyberintimidation/cyberintimidation-illegale.html (consulté en août 2021).

SP – Sécurité publique Canada, 2021b. Réunion ministérielle des cinq pays. Adresse : https://www.securitepublique.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-fr.aspx (consulté en septembre 2021).

SP – Sécurité publique Canada, 2021c. La traite des personnes, ce n'est pas ce que vous pensez. Adresse : https://www.canada.ca/fr/securite-publique-canada/campagnes/traite-des-personnes.html (consulté en août 2021).

Spencer, D. C., R. Ricciardelli, D. Ballucci, et K. Walby, 2020. « Cynicism, dirty work, and policing sex crimes », *Policing: An International Journal*, vol. 43, n°1, p. 151-165.

Starr, P., 2005. *The Creation of the Media: Political Origins of Modern Communications*. New York, NY, Basic Books.

StatCan – Statistique Canada, 2001. Enquête sur l'utilisation d'Internet par les ménages. Adresse : https://www150.statcan.gc.ca/n1/daily-quotidien/020725/dq020725a-fra.htm (consulté en mai 2022).

StatCan – Statistique Canada, 2018. Langue – Faits saillants en tableaux, Recensement de 2016. Adresse : https://www12.statcan.gc.ca/census-recensement/2016/dp-pd/hlt-fst/lang/Tableau.cfm?Lang=F&T=31&Geo=00&SP=1&view=2&age=1&rl=1 (consulté en avril 2022).

StatCan – Statistique Canada, 2020a. Les Canadiens dépensent plus d'argent et passent plus de temps en ligne pendant la pandémie, et plus des deux cinquièmes ont déclaré un cyberincident. Adresse : https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-fra.htm (consulté en août 2020).

StatCan – Statistique Canada, 2020b. Les ressources policières au Canada, 2019. Adresse : https://www150.statcan.gc.ca/n1/pub/85-002-x/2020001/article/00015-fra.htm (consulté en octobre 2022).

StatCan – Statistique Canada, 2021a. *Enquête canadienne sur l'utilisation d'Internet, 2020*, Ottawa, ON, StatCan.

StatCan – Statistique Canada, 2021b. Cybercrimes déclarés par la police, selon l'infraction reliée à la cybercriminalité, Canada (certains services de police). Adresse : https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=3510000101&request_locale=fr (consulté en août 2021).

StatCan – Statistique Canada, 2021c. *Cybercrime: Changes to the Uniform Crime Reporting Survey (UCR 2.4)*, Ottawa, ON, StatCan.

StatCan – Statistique Canada, 2022. Statistiques des crimes fondés sur l'affaire, par infractions détaillées, Canada, provinces, territoires, régions métropolitaines de recensement et Police militaire des Forces canadiennes. Adresse : https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=3510017701&pickMembers%5B0%5D=1.1&pickMembers%5B1%5D=2.257&cubeTimeFrame.startYear=2010&cubeTimeFrame.endYear=2021&referencePeriods=20100101%2C20210101&request_locale=fr (consulté en octobre 2022).

Stecula, D. A. et M. Pickup, 2021. « Social media, cognitive reflection, and conspiracy beliefs », *Frontiers in Political Science*, vol. 3, p. 62.

Steeves, V., 2009. « Reclaiming the Social Value of Privacy », dans Kerr, I., V. Steeves et C. Lucock(réd.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, NY, Oxford University Press.

Stigall, M. et K.-K. R. Choo, 2021. « Digital Forensics Education: Challenges and Future Opportunities », dans Choo, K.-K. R., T. Morris, G. Peterson et E. Imsand(réd.), *National Cyber Summit (NCS) Research Track*, vol. 310, Cham, Switzerland, Springer.

Stoddart, J., 2004. Élaborer une approche canadienne en matière de protection de la vie privée. Adresse : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2004/sp-d_041119/ (consulté en juin 2022).

Stoddart, J., 2007. La Charte et la sécurité. Adresse : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2007/sp-d_070216/ (consulté en mai 2022).

Stoltz, M., A. Crocker, et C. Schmon, 2022. The EU Digital Markets Act's Interoperability Rule Addresses an Important Need, but Raises Difficult Security Problems for Encrypted Messaging. Adresse : https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises (consulté en mai 2022).

Strawhun, J., N. Adams, et M. T. Huss, 2013. « The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse », *Violence and Victims*, vol. 28, n°4, p. 141-156.

Suares, W., 2019. Experts Advise Protecting Yourself Against Stalking in the Digital Age. Adresse : https://okcfox.com/news/local/stalking-in-the-digital-age (consulté en octobre 2022).

Sullivan, D., 2021. Giving Kids and Teens More Control over Their Images in Search. Adresse : https://blog.google/products/search/giving-kids-and-teens-more-control-over-their-images-search/ (consulté en octobre 2022).

Swartz, K., 2021. Mapping Out How Decentralised Exchanges Can be Regulated. Adresse : https://www.regulationasia.com/mapping-out-how-decentralised-exchanges-can-be-regulated/ (consulté en février 2022).

Swire-Thompson, B. et D. Lazer, 2020. « Public health and online misinformation: Challenges and recommendations », *Annual Review of Public Health*, vol. 41, p. 433-451.

Talbot, M., 2021. Canadian Civil Liberties Association has 'serious concerns' about CCTV Expansion in Ontario. Adresse : https://toronto.citynews.ca/2021/07/13/cctv-cameras-privacy-ontario/ (consulté en août 2021).

Tanner, S. et A. Campana, 2020. « "Watchful citizens" and digital vigilantism: A case study of the far right in Quebec », *Global Crime*, vol. 21, n°3-4, p. 262-282.

Taylor, S., 2017. More Inmates in Sask.'s Jails, Shortage of Crown Prosecutors in Regina. Adresse : https://www.cbc.ca/news/canada/saskatchewan/saskatchewan-justice-ministry-extra-costs-1.4441589 (consulté en avril 2022).

Tcherni, M., A. Davies, G. Lopes, et A. Lizotte, 2016. « The dark figure of online property crime: Is cyberspace hiding a crime wave? », *Justice Quarterly*, vol. 33, n°5, p. 890-911.

Tenove, C., H. J. S. Tworek, et F. McKelvey, 2018. *Poisoning Democracy: How Canada Can Address Harmful Speech Online*, Ottawa, ON, Forum des politiques publiques.

Tenove, C. et H. Tworek, 2019. « Online disinformation and harmful speech: Dangers for democratic participation and possible policy responses », *Journal of Parliamentary & Political Law*, vol. 13, p. 215-232.

Tenove, C. et H. Tworek, 2020. *Trolled on the Campaign Trail: Online Incivility and Abuse in Canadian Politics*, Vancouver (BC), University of British Columbia's Centre for the Study of Democratic Institutions.

Terrill, R. J., 2013. *World Criminal Justice Systems. A Comparative Survey.* Waltham, MA, Anderson Publishing.

The Canadian Press, 2021. Canadian Companies Hit by Ransomware Attacks Pay Almost $500,000 on Average to Perpetrators, Survey Finds. Adresse : https://www.theglobeandmail.com/business/article-canadian-companies-hit-by-ransomware-attacks-pay-almost-500000-on/ (consulté en mai 2022).

The eQuality Project, s.d. How Do Administrative & Regulatory Law Respond to Tech-Facilitated Violence? Adresse : https://www.equalityproject.ca/resources/legal-briefs-answering-your-questions-about-cyberbullying-law/legal-briefs-how-do-administrative-regulatory-law-respond-to-cyberviolence/#_ftn2 (consulté en avril 2022).

Theocharis, Y., A. Cardenal, S. Jin, T. Aalberg, D. N. Hopmann, J. Strömbäck, … V. Štětka, 2021. « Does the platform matter? Social media and COVID-19 conspiracy theory beliefs in 17 countries », *New Media & Society*, 14614448211045666.

Therrien, D., 2021a. Examining the Canadian Competition Act in the Digital Era. Adresse : https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_sen-ont_211221/ (consulté en juin 2022).

Therrien, D., 2021b. The Future of Privacy Law Reform in Canada: Remarks at the IAPP Canada Privacy Symposium 2021. Adresse : https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210526/ (consulté en mai 2022).

Thiessen, B., A. LaRoche, et J. Lee, 2021. Tort of 'Public Disclosure of Private Facts' Recognized in Alberta in 'Revenge Porn' Case. Adresse : https://www.osler.com/en/resources/regulations/2021/tort-of-public-disclosure-of-private-facts-recognized-in-alberta-in-revenge-porn-case (consulté en mai 2022).

Thompson, E., 2022. Convoy Protest Could Change the Way Money is Monitored, Says Watchdog Agency. Adresse : https://www.cbc.ca/news/politics/truck-convoy-fundraiser-gofundme-1.6346639 (consulté en mars 2022).

Thompson, S. et D. Lyon, 2021. « Pixies, Pop-Out Intelligence, and Sandbox Play: The New Analytic Model and National Security Surveillance in Canada », dans Lyon, D. et D. Murakami Wood(réd.), *Big Data Surveillance and Security Intelligence: The Canadian Case*, Vancouver, BC, University of British Columbia Press.

Tile, 2022. Tile's Scan and Secure Feature Addresses Unwanted Tracking. Adresse : https://www.tile.com/en-us/blog/tile-introduces-scan-and-secure-feature-unwanted-tracking-safety (consulté en octobre 2022).

Tile, s.d. How Tile Works. Adresse : https://www.tile.com/en-CA/how-it-works (consulté en octobre 2022).

Titley, G., E. Keen, et L. Foldi, 2014. *Starting Points for Combatting Hate Speech Online*, Strasbourg, France, Council of Europe, Youth Division.

TMU – Université métropolitaine de Toronto, 2022. Cybersecurity, Data Protection and Digital Forensics. Adresse : https://continuing.torontomu.ca/public/category/courseCategoryCertificateProfile.do?method=load&certificateId=170590 (consulté en juin 2022).

Tolosana, R., R. Vera-Rodriguez, J. Fierrez, A. Morales, et J. Ortega-Garcia, 2020. « Deepfakes and beyond: A survey of face manipulation and fake detection », *Information Fusion*, vol. 64, p. 131-148.

TPSB – Toronto Police Services Board, 2022. Use of Artifical Intelligence Technology. Adresse : https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology (consulté en juin 2022).

Triggs, G., 2019. Why an Australian Charter of Rights is a Matter of National Urgency. Adresse : https://theconversation.com/why-an-australian-charter-of-rights-is-a-matter-of-national-urgency-121411 (consulté en janvier 2022).

Tripp, H., 2019. « All sex workers deserve protection: How FOSTA/SESTA overlooks consensual sex workers in an attempt to protect sex trafficking victims », *Penn State Law Review*, vol. 124, n°1, article 6.

Trudel, P., 2021. « Fausses nouvelles et réseaux sociaux », dans Hervé, C. et M. Stanton-Jean(réd.), *Éthique, intégrité scientifique et fausses nouvelles*, PFranceFrance, Dalloz.

Tsekouras, P., 2021. Apple Tracking Devices Being Used in Thefts of High-End Cars in York Region: Pol ce. Adr esse : https://toronto.ctvnews.ca/apple-tracking-devices-being-used-in-thefts-of-high-end-cars-in-york-region-police-1.5690819 (consulté en mars 2022).

Tsui, J., 2020. Why Gender-Neutral Facial Recognition Will Change How We Look at Technol gy. Adr esse : https://www.technologynetworks.com/informatics/articles/why-gender-neutral-facial-recognition-will-change-how-we-look-at-technology-332962 (consulté en avril, 2022).

Tunney, C., 2022. Federal Government Invokes Emergencies Act for First Time Ever in Response to Protests, Blocka es. Adr esse : https://www.cbc.ca/news/politics/trudeau-premiers-cabinet-1.6350734 (consulté en avril 2022).

Twitter, 2021a. An Update Following the Riots in Washington, DC. Adr esse : https://blog.twitter.com/en_us/topics/company/2021/protecting--the-conversation-following-the-riots-in-washington-- (consulté en novembre 2021).

Twitter, 2021b. Our Range of Enforcement Opti ns. Adr esse : https://help.twitter.com/en/rules-and-policies/enforcement-options (consulté en août 2021).

Tworek, H. et P. Leerssen, 2019. *An Analysi' of Germany's NetzDG Law*, Philadelphia, PA, Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression.

Tworek, H., 2020. *How a Public Health Approach Could Help Curb the Infodemic*, Waterloo, ON, Centre for International Governance Innovation.

Tworek, H., 2021a. History Explains Why Global Content Moderation Cannot Work. Adresse : https://www.brookings.edu/techstream/history-explains-why-global-content-moderation-cannot-work/ (consulté en mars 2022).

Tworek, H., 2021b. « Fighting hate with speech law: Media and German visions of democracy », *The Journal of Holocaust Research*, vol. 35, p. 106-122.

Tworek, H., 2022. *Authorities Were Warned about Extremist Fundraising Online but Did Not Seem to Hear*, Waterloo, ON, Centre for International Governance Innovation.

Tworek, H. et Wanless, A., 2022. Time for Transparency From Digital Platforms, But What Does That Really Mean? Adresse : https://www.lawfareblog.com/time-transparency-digital-platforms-what-does-really-mean (consulté en mars 2022).

UE – Union européenne, 2000. *Directive 2000/31/CE du parlement Européen et du conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»)*, Bruxelles, Belgique, Parlement européen et Conseil de l'Union européenne.

UE – Union européenne, 2016. *Règlements (UE) 2016/679 du parlement Européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, Bruxelles, Belgique, Parlement européen et Conseil de l'Union européenne.

Ullmann, S. et M. Tomalin, 2020. « Quarantining online hate speech: Technical and ethical perspectives », *Ethics and Information Technology*, vol. 22, p. 69-80.

UN News – United Nations News, 2020. Online Predators Put Millions of Children at Risk During COVID-19 Pandemic Shutdown. Adresse : https://news.un.org/en/story/2020/04/1061742 (consulté en août 2021).

UNESCO – United Nations Le journalisme, « les fausses nouvelles » (fake news) et désinformation : un manuel pour l'enseignement et la formation du journalisme. Adresse : https://fr.unesco.org/fightfakenews (consulté en juin 2022).

Uscinski, J. E. et J. M. Parent, 2014. « Who Are the Conspiracy Theorists? », dans Uscinski, J. E. et J. M. Parent(réd.), *American Conspiracy Theories*, New York, NY, Oxford University Press.

Vaccari, C. et A. Chadwick, 2020. « Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news », *Social Media + Society*, vol. 6, n°1, 2056305120903408.

Van Cauwenberghe, C., 2015. Canada: Amendments to PIPEDA Give Financial Institutions New Artillery in Fighting Financial Abuse. Adresse : https://www.mondaq.com/canada/financial-services/438616/amendments-to-pipeda-give-financial-institutions-new-artillery-in-fighting-financial-abuse (consulté en octobre 2022).

Van Puyvelde, D., S. Coulthart, et M. S. Hossain, 2017. « Beyond the buzzword: Big data and national security decision-making », *International Affairs*, vol. 93, n°6, p. 1397-1416.

Velásquez, N., R. Leahy, N. Johnson Restrepo, Y. Lupu, R. Sear, N. Gabriel, ... N. F. Johnson, 2021. « Online hate networks spreads malicious COVID-19 content outside the control of individual social media platforms », *Scientific Reports*, vol. 11, 11549

Vidal-Tomás, D., 2022. « Which cryptocurrency data sources should scholars use? », *International Review of Financial Analysis*, vol. 81, 102061.

Vigderman, A. et G. Turner, 2022. 2022 VPN Usage Statistics. Adresse : https://www.security.org/vpn/statistics/ (consulté en octobre 2022).

Ville de Calgary, 2021. Calgary Police Service and RCMP Contribute to Ransomware Arrests and Seizures Overseas in Operation GoldDust. Adresse : https://newsroom.calgary.ca/calgary-police-service-and-rcmp-contribute-to-ransomware-arrests-and-seizures-overseas-in-operation-golddust/ (consulté en janvier 2022).

Vincent, J., 2020. Twitter is bringing its 'Read Before you Retweet' Prompt to All Users. Adresse : https://www.theverge.com/2020/9/25/21455635/twitter-read-before-you-tweet-article-prompt-rolling-out-globally-soon (consulté en juin 2021).

Vincze, E. A., 2016. « Challenges in digital forensics », *Police Practice and Research*, vol. 17, n°2, p. 183-194.

von Sikorski, C., 2021. « Visual polarisation: Examining the interplay of visual cues and media trust on the evaluation of political candidates », *Journalism*, vol. 23, n°9, p. 1900-1918.

Vosoughi, S., D. Roy, et S. Aral, 2018. « The spread of true and false news online », *Science*, vol. 359, n°6380, p. 1146-1151.

Wachter, S. et B. Mittelstadt, 2019. « A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI », *Columbia Business Law Review*, vol. 2019, n°2, p. 494-620.

Wagner, A., 2022. « Tolerating the trolls? Gendered perceptions of online harassment of politicians in Canada », *Feminist Media Studies*, p. 1-16.

Waldman, A. E., 2018. *Privacy as Trust: Information Privacy for an Information Age*. Cambridge, UK, Cambridge University Press.

Walker, J., 2018. *Discours haineux et liberté d'expression : balises légales au Canada*, Ottawa, ON, Bibliothèque du Parlement.

Waller, I. et A. Anderson, 2021. « Quantifying social organization and political polarization in online platforms », *Nature*, vol. 600, n°7888, p. 264-268.

Walter, M., T. Kuktai, S. R. Carroll, et D. Rodriguez-Lonebear, 2020. *Indigenous Data Sovereignty and Policy*. Londres, Royaume-Uni, Routledge.

Wanamaker, K., 2019. *Profil des entreprises canadiennes qui signalent les cybercrimes à la police : L'Enquête canadienne sur la cybersécurité et le cybercrime de 2017*, Ottawa, ON, Sécurité publique Canada.

Wang, J., T. R. Nansel, et R. J. Iannotti, 2011. « Cyber bullying and traditional bullying: Differential association with depression », *Journal of Adolescent Health*, vol. 48, n°4, p. 415-417.

Watson, C. et L. Huey, 2020. « Technology as a source of complexity and challenge for special victims unit (SVU) investigators », *International Journal of Police Science & Management*, vol. 22, n°4, p. 419-427.

Weaver, N., 2021. The Ransomware Problem Is a Bitcoin Problem. Adresse : https://www.lawfareblog.com/ransomware-problem-bitcoin-problem (consulté en juin 2022).

Weimann, G., 2016. « Terrorist migration to the dark web », *Perspectives on Terrorism*, vol. 10, n°3, p. 40-44.

Wells, R., 2019. The Trauma of Revenge Porn. Adresse : https://www.nytimes.com/2019/08/04/opinion/revenge-porn-privacy.html (consulté en décembre 2022).

Wells, R., s.d.-a. Bekah Wells Attorney-at-Law. Adresse : https://www.bekahwells.com/ (consulté en février 2022).

Wells, R., s.d.-b. Women Against Cyberrape. Adresse : https://www.womenagainstcyberrape.com/ (consulté en février 2022).

West, L. et C. Forcese, 2020. « Twisted into knots: Canada's challenges in lawful access to encrypted communications », *Common Law World Review*, vol. 49, n°3-4, p. 182-198.

Westlake, B., M. Bouchard, et R. Frank, 2012. *Comparing Methods for Detecting Child Exploitation Content Online*, communication présentée dans le cadre du European Intelligence and Security Informatics Conference, Odense, Denmark.

Willey, J., 2018. Houston Woman Says Ex Used 'Tile' Device to Stalk Her Repeatedly. Adresse : https://abc13.com/houston-woman-harassment-high-tech-device-stalking/3719155/ (consulté en octobre 2022).

Williams, M. L., P. Burnap, A. Javed, H. Liu, et S. Ozalp, 2020. « Hate in the machine: Anti-black and anti-muslim social media posts as predictors of offline racially and religiously aggravated crime », *British Journal of Criminology*, vol. 60, n°1, p. 93-117.

Williams, T., 2017. Backpage's Sex Ads are Gone. Child Trafficking? Hardly. Adresse : https://www.nytimes.com/2017/03/11/us/backpage-ads-sex-trafficking.html (consulté en décembre 2022).

Windwehr, S. et J. C. York, 2020. Facebook's Most Recent Transparency Report Demonstrates the Pitfalls of Automated Content Moderation. Adresse : https://www.eff.org/deeplinks/2020/10/facebooks-most-recent-transparency-report-demonstrates-pitfalls-automated-content (consulté en novembre 2021).

Winner, L., 1980. « Do Artifacts Have Politics? », *Daedalus*, vol. 109, n°1, p. 121-136.

Winter, J., 2019. FBI Document Warns Conspiracy Theories Are a New Domestic Terrorism Threat. Adresse : https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cubnl0aW1lc%E2%80%A6 (consulté en novembre 2021).

Wright, J. M., W. H. K. Chun, A. Clarke, M. Herder, et H. P. Ramos, 2022. *Protecting Expert Advice for the Public: Promoting Safety and Improved Communications*, Ottawa, ON, Royal Society of Canada.

Yar, M. et J. Drew, 2019. « Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales », *International Journal of Cyber Criminology*, vol. 12, n°2, p. 578-594.

YouTube, 2019. Continuing Our Work to Improve Recommendations on YouTube. Adresse : https://blog.youtube/news-and-events/continuing-our-work-to-improve/ (consulté en novembre 2021).

YRP – Police régionale de York, 2021. Vehicle Theft Warning and Prevention Tips. Adresse : https://www.yrp.ca/en/Modules/News/index.aspx?newsId=167fa5b3-3583-431d-8cc0-91e49aee3bff (consulté en janvier 2022).

Završnik, A., 2020. « Criminal justice, artificial intelligence systems, and human rights », *ERA Forum*, vol. 20, n°4, p. 567-583.

Zimmer, K., 2022. *Utilizing the Courts for an Online Reputational Scrub, and the Potential Emergence of a Right to Be Forgotten in Canada*, Vancouver, BC, Continuing Legal Education Society of British Columbia.

Rapports utiles du CAC

Les rapports d'évaluation répertoriés ci-dessous sont accessibles sur le site Web du CAC (www.rapports-cac.ca) :

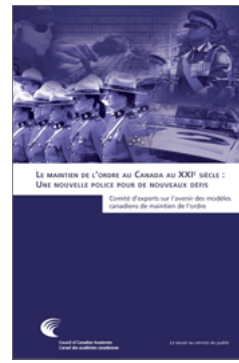
Lignes de faille (2023)

Entre progrès et défis (2022)

En attente de connexion (2021)

Vers la paix, l'harmonie et le bien-être : Les services de police dans les communautés autochtones (2019)

L'accès aux données sur la santé et aux données connexes au Canada (2015)



Le maintien de l'ordre au Canada au XXIe siècle : Une nouvelle police pour de nouveaux défis (2014)

Conseil d'administration*

Chantal Guay (présidente par intérim), FACG, directrice générale, Conseil canadien des normes (Ottawa, Ont.)

Soheil Asgarpour, FACG, président, Petroleum Technology Alliance Canada; président désigné, Académie canadienne du génie (Calgary, Alb.)

Pascal Grenier, Vice-président principal, Services de vol et Opérations mondiales, CAE (Montréal, Qc)

Judy Illes, C.M., MACSS, MSRC, professeure et éminente chercheuse, Université de la Colombie-Britannique (Vancouver, C.-B.)

Jawahar (Jay) Kalra, M.D., MACSS, professeur, Département de pathologie et de médecine de laboratoire et membre du Conseil des gouverneurs, Université de la Saskatchewan (Saskatoon, Sask.)

Catherine Karakatsanis, FACG, cheffe de l'exploitation, Morrison Hershfield Group Inc. et présidente élue de l'Académie canadienne du génie (Toronto, Ont.)

Cynthia E. Milton, MSRC, vice-présidente associée à la recherche, Université de Victoria (Victoria, C.-B.)

Sue Molloy, FACG, présidente de Glas Ocean Electric et professeure auxiliaire à l'Université Dalhousie (Halifax, N.-É.)

Donna Strickland, C.C., MSRC, FACG, professeure, Département de physique et d'astronomie, Université de Waterloo (Waterloo, Ont.)

Gisèle Yasmeen, agrégée superior, Institute of Asian Research, School of Public Policy and Global Affairs, Université de la Colombie-Britannique (Vancouver, C.-B.)

*Au 1er mars 2023

Comité consultatif scientifique*

David Castle (président), professeur, École d'administration publique et Gustavson School of Business; chercheur en résidence, Bureau du conseiller scientifique principal du premier ministre du Canada (Victoria, C.-B.)

Maydianne C. B. Andrade, professeure de sciences biologiques, Université de Toronto à Scarborough; présidente, Réseau canadien des scientifiques noirs, Toronto, Ont.)

Peter Backx, MSRC, professeur, Département de biologie; titulaire, Chaire de recherche du Canada en biologie cardiovasculaire, Université York (Toronto, Ont.)

Kyle Bobiwash, professeur adjoint, érudit autochtone, Entomologie, Université du Manitoba (Winnipeg, Man.)

Stephanie E. Chang, professeure, School of Community and Regional Planning and Institute for Resources, Environment and Sustainability, Université de la Colombie-Britannique (Vancouver, C.-B.)

Jackie Dawson, titulaire de la Chaire de recherche du Canada sur l'environnement, la société et les politiques et professeure agrégée au Département de géographie, Université d'Ottawa (Ottawa, Ont.)

Colleen M. Flood, MSRC, MACSS, directrice, Centre de droit, politique et éthique de la santé; professeure, Faculté de droit (section droit commun), Université d'Ottawa (Ottawa, Ont.)

Digvir S. Jayas, O.C., MSRC, FACG, professeur éminent et vice-recteur à la recherche et aux relations internationales, Université du Manitoba (Winnipeg, Man.)

Malcolm King, MACSS, directeur scientifique, Saskatchewan Centre for Patient-Oriented Research, Université de la Saskatchewan (Saskatoon, Sask.)

Chris MacDonald, professeur agrégé; directeur, Ted Rogers Leadership Centre; président, Département de droit et des affaires; Ted Rogers School of Management, l'Université métropolitaine de Toronto (Toronto, Ont.)

Nicole A. Poirier, FACG, présidente, KoanTeknico Solutions Inc. (Beaconsfield, Qc)

Louise Poissant, MSRC, directrice scientifique du Fonds de recherche du Québec – Société et culture (Montréal, Qc)

Jamie Snook, directeur général, Torngat Wildlife Plants and Fisheries Secretariat (Happy Valley-Goose Bay, T.-N.-L.)

David A. Wolfe, professeur de sciences politiques, Université de Toronto à Mississauga; codirecteur, Innovation Policy Lab à la Munk School of Global Affairs and Public Policy, Université de Toronto (Toronto, Ont.)

*Au 1er mars 2023

Council of Canadian Academies | Conseil des académies canadiennes

180, rue Elgin, bureau 1401
Ottawa (Ontario) K2P 2K3
Tél: 613 567-5000
www.rapports-cac.ca