Bureau de l'ombudsman fédéral des victimes d'actes criminels
Office of the Federal Ombudsman for Victims of Crime

Écoutées. Respectées. **Les victimes d'abord.**
Heard. Respected. **Victims First.**

Le point de vue des victimes : Combler les besoins des victimes dans le contexte de la cybercriminalité et de ses effets

Mémoire soumis dans le cadre de la consultation de Sécurité publique Canada sur la cybersécurité

Présenté par Sue O'Sullivan,
ombudsman fédérale des victimes d'actes criminels
Octobre 2016

Canada

Table des matières

Le Bureau de l'ombudsman fédéral des victimes d'actes criminels

Ressource indépendante pour les victimes au Canada, le Bureau de l'ombudsman fédéral des victimes d'actes criminels (BOFVAC) a été créé en 2007 afin d'assurer que le gouvernement du Canada s'acquitte de ses responsabilités à l'égard des victimes d'actes criminels.

Notre mandat porte exclusivement sur des questions de compétence fédérale et consiste notamment à :

- promouvoir l'accès des victimes aux programmes et aux services fédéraux existants qui les concernent;
- répondre aux plaintes de victimes au sujet du non-respect des dispositions de la *Loi sur le système correctionnel et la mise en liberté sous condition* qui s'appliquent aux victimes d'actes criminels perpétrés par des délinquants relevant des autorités fédérales;
- sensibiliser le personnel et les décideurs du système de justice pénale aux besoins et aux préoccupations des victimes ainsi qu'aux lois qui aident les victimes, notamment en appliquant les principes énoncés dans la *Déclaration canadienne des principes fondamentaux de justice relatifs aux victimes de la criminalité* dans les domaines de compétence fédérale;
- relever et examiner les nouveaux enjeux et les problèmes systémiques, notamment ceux qui sont liés aux programmes et aux services que fournissent ou administrent le ministère de la Justice ou le ministre de la Sécurité publique et de la Protection civile et qui ont une incidence négative sur les victimes d'actes criminels;
- faciliter l'accès des victimes aux programmes et aux services fédéraux existants en leur fournissant des renseignements et des services d'aiguillage.

En outre, nous discutons avec le gouvernement de l'incidence de la *Charte canadienne des droits des victimes* (CCDV) sur notre mandat. La CCDV donne aux victimes d'actes criminels qui se sont inscrites auprès du Service correctionnel du Canada (SCC) ou de la Commission nationale des libérations conditionnelles une voix plus efficace au sein du système de justice pénale, en donnant à ces victimes,

des droits à l'information, à la protection, à la participation et à un dédommagement ainsi qu'à des recours[1].

Une part importante du travail du BOFVAC consiste à amplifier la voix des victimes d'actes criminels au Canada en nous assurant que les victimes seront **informées, considérées, protégées et soutenues.** C'est pourquoi le BOFVAC se réjouit d'avoir l'occasion de fournir son apport à la consultation de Sécurité publique Canada sur la cybersécurité.

[1] Toute victime qui estime qu'un organisme fédéral a contrevenu à l'un de ses droits garantis par la CCDV, ou l'a privée d'un tel droit, peut déposer une plainte.

Introduction

Chaque jour, le cybermilieu fait des victimes au Canada. Cette victimisation prend différentes formes[2] et elle peut avoir des répercussions graves et durables pour les personnes qu'elle blesse et leurs êtres chers.

Après avoir écouté les points de vue de victimes, d'organismes de services aux victimes et de spécialistes de la cybercriminalité et de la cybervictimisation, nous pensons qu'une optique des victimes doit être appliquée au renouvellement de la stratégie canadienne en matière de cybersécurité. Pour nous attaquer à des enjeux comme la prévention ou la dissuasion, nous devons travailler à rebours afin de déterminer *explicitement* ce que nous voulons prévenir. Si nous voulons établir une vaste stratégie visant à assurer la santé et la sécurité des collectivités, nous devons faire une place de choix à la prévention non seulement par rapport à la perpétration de l'acte criminel lui-même, mais aussi par rapport à ses répercussions durables et à tout autre préjudice ou traumatisme qu'une victime pourrait subir au long de son cheminement dans le système de justice pénale. Si nous voulons réduire les préjudices et maximiser la résilience dans le sillage d'un acte criminel, nous devons être prêts à envisager, dès le départ, les besoins et les préoccupations des victimes d'actes criminels, à en tenir compte et à les mettre à l'avant-plan lors de l'élaboration de programmes, de politiques, de lois et de stratégies. En plaçant le point de vue des victimes au cœur de la conversation, nous contribuerons au respect de leurs droits et de leurs besoins, à leur accès à des mesures de soutien et à des services pertinents et à leur pouvoir de dénoncer la cybercriminalité et de participer à part entière au système de justice pénale.

À cette fin, nous présentons dans le présent mémoire le contexte de la cybervictimisation et son importance dans le cadre de la cybersécurité dans son ensemble. Nous formulons aussi des recommandations sur cinq domaines « fondamentaux » relatifs à la cybervictimisation : **données et statistiques**; **sensibilisation du public et formation**; **mesures de soutien axées sur la victime**; **partenariats multisectoriels**; et **lois**.

[2] La cybervictimisation consiste en différents incidents qui sont des infractions criminelles sous le régime du *Code criminel* et en d'autres incidents qui n'en sont pas.

Contexte

Qu'est-ce que la cybervictimisation?

Quand nous examinons la cybersécurité et les cybermenaces, notre objectif, à terme, est d'éviter la victimisation et ses répercussions. La cybervictimisation prend différentes formes, notamment la cyberintimidation[3], le harcèlement électronique, la fraude bancaire et par carte de crédit sur Internet et l'usurpation d'identité.

En outre, de jeunes Canadiens et Canadiennes – y compris des enfants – et des adultes sont victimes de différents types de cyberviolence sexuelle, qui peuvent prendre différentes formes. La distribution d'enregistrements, d'images ou de messages sexuels sans consentement en constitue un exemple. Dans certains cas, l'image distribuée est celle d'une agression sexuelle tandis que dans d'autres cas, elle illustre des actes sexuels consensuels. Cela peut aussi comprendre la « pornographie de vengeance », qui renvoie à la diffusion en ligne d'images intimes sans le consentement de la personne concernée, le plus souvent par un ancien partenaire intime qui veut l'humilier et lui faire du tort. Voici d'autres exemples de cyberviolence sexuelle : le leurre en ligne et l'exploitation sexuelle en ligne de mineurs par des adultes qui communiquent avec eux dans le but de commettre une infraction d'ordre sexuel; la « sextorsion », dans le cadre de laquelle les victimes sont menacées de la distribution en ligne d'images ou de renseignements sexuels, parfois avec la réserve supplémentaire que les victimes peuvent « éviter » la distribution de ce matériel si elles se livrent à certaines activités sexuelles ou illégales; et l'agression sexuelle virtuelle, dans laquelle une victime reçoit en ligne des menaces d'agression sexuelle d'une ou de plusieurs personnes.

Vu la nature changeante de l'environnement en ligne, d'autres formes de victimisation se dessinent. Par exemple, on voit de plus en plus l'utilisation d'Internet pour recruter les victimes potentielles de la traite d'humains ou attirer des personnes dans un endroit donné pour les voler.

---

[3] La cyberintimidation « consiste à utiliser les technologies de communication telles qu'Internet, les sites de réseautage social, les sites Web, le courriel, la messagerie texte et la messagerie instantanée pour intimider une personne à répétition ou la harceler ». En voici des exemples : envoyer des courriels ou des messages textes ou instantanés méchants ou menaçants; ou amener une personne à révéler des renseignements personnels ou des choses gênantes puis les transmettre à d'autres. http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-fra.htm

La cybervictimisation par opposition à des formes « conventionnelles » de victimisation

La cybercriminalité change la dynamique traditionnelle entre délinquants et victimes. Des chercheurs ont décrit les caractéristiques propres à l'environnement en ligne qui distinguent la cybervictimisation des formes conventionnelles de victimisation[4], notamment :

- **Accessibilité accrue** – Alors que, dans le passé, les prédateurs devaient avoir accès à leurs victimes ou se trouver près d'elles, ils peuvent désormais ouvrir une session et avoir accès à des milliers, voire des millions de victimes à tout moment. Les domaines d'accès sont aussi beaucoup plus vastes. Par exemple, alors que les prédateurs sexuels devaient autrefois se replier sur des forums relativement peu nombreux (écoles, sports, etc.), les plateformes au moyen desquelles ils peuvent contacter des victimes sont beaucoup plus nombreuses et comprennent les salons de clavardage, les plateformes de jeux, les réseaux sociaux et bien d'autres encore. Le monde en ligne n'est pas limité par des contraintes de temps typiques; un préjudice peut être infligé 24 heures par jour, sept jours par semaine.

- **Anonymat ou déguisement** – La victimisation peut avoir lieu à une échelle mondiale, tandis que leurs auteurs conservent un anonymat relatif. Cet anonymat fait en sorte que des agresseurs peuvent aussi trouver plus facile de se montrer cruels puisqu'ils ne peuvent pas voir leurs victimes ou être vus par elles. Cet anonymat peut aussi permettre à des prédateurs de se déguiser, se faisant passer pour des personnes du sexe opposé, ou plus jeunes, ce qui peut encourager des enfants à se montrer plus ouverts et confiants lorsqu'ils divulguent des renseignements ou organisent une rencontre.

[4] Voir, par exemple, Kiriakidis, S. et Kavoura, A., 2010, « Cyberbullying : A review of the literature on harassment through the internet and other electronic means ». *Family and Community Health*, *33*(2), p. 82-93; Hinduja, S. et Patchin, J.W., 2014, Cyberbullying Identification, Prevention and Response (Cyberbullying Research Center) document consulté le 22 septembre 2016 à l'adresse suivante : http://cyberbullying.org/Cyberbullying-Identification-Prevention-Response.pdf,.

- **Détectabilité** – Tandis que le vol ou les agressions conventionnelles laissent des traces physiques, dans certains incidents de cybercriminalité, il peut arriver que les victimes ne s'aperçoivent qu'après coup qu'elles ont été victimisées. Il pourrait s'agir d'incidents dans lesquels des images de nature sexuelle d'une personne sont diffusées sur Internet sans son consentement, ou de victimes à qui de l'argent a été volé.
- **Rapidité et impossibilité de limiter** – La vitesse avec laquelle des images peuvent être diffusées est étonnante et, malheureusement, il est souvent impossible de les retracer et de les supprimer entièrement. Des remarques cruelles peuvent inonder un site Web en quelques minutes et une usurpation d'identité ou la fraude financière peut découler de la réponse à un seul courriel d'hameçonnage.

Conjugués à la nature complexe et changeante de l'univers en ligne, ces facteurs, entre autres, font en sorte qu'il est particulièrement difficile de prévoir et de prévenir la cybervictimisation, ou qu'elle fasse l'objet d'une enquête ou de poursuites.

Conséquences de la cybervictimisation

Bien que la cybercriminalité soit parfois vue comme distante, intangible ou même « dépourvue de victimes », la victimisation et les conséquences qui en découlent sont réelles et importantes.

L'International Centre for Criminal Law Reform and Criminal Justice Policy [Centre pour la réforme du droit criminel et la politique en matière de justice] a reconnu que les délits liés à l'identité figurent [TRADUCTION] « parmi les crimes économiques les plus graves et dont la croissance est la plus rapide en Amérique du Nord[5] ». En 2013, le Centre antifraude du Canada a fait état de plus de 52 millions de dollars de pertes dues à la fraude par marketing de masse et environ 11 millions de dollars de pertes dues à la fraude liée à l'identité. En 2014, la cybercriminalité déclarée par la police au Canada consistait en des crimes graves comme le harcèlement criminel, la

[5] International Centre for Criminal Law Reform and Criminal Justice Policy, 2011, Responding to Victims of Identity Crime : A Manual for Law Enforcement Agents, Prosecutors and Policy-makers, consulté le 4 octobre 2016.

pédopornographie, les menaces, l'exploitation sexuelle et le leurre d'un enfant[6]. En outre, la fraude liée à l'identité et la pédopornographie – deux crimes généralement associés de nos jours avec l'utilisation d'Internet et des technologies de l'information – figurent parmi les rares crimes déclarés par la police dont le nombre et la gravité ont augmenté entre 2013 et 2014[7].

Il est important de ne pas oublier que la cybercriminalité n'est pas un crime sans victime. Comme d'autres formes de victimisation, elle entraîne des conséquences néfastes. Par exemple, les victimes de fraude liée à l'identité en ligne peuvent subir une gamme de préjudices, notamment des pertes financières directes (biens, services ou argent perdus au profit de la personne qui a détourné le compte ou les renseignements personnels de la victime), le harcèlement par des créanciers ou des agents de recouvrement, la perte de revenus ou de possibilités économiques en raison d'une réputation financière ternie (p. ex., incapacité d'obtenir du crédit par suite d'une fraude ou d'une identité corrompue, ou perte d'un emploi), la perte de la confiance de sa famille et de son entourage par suite d'une réputation entachée, le traumatisme et la dépression[8].

La cyberviolence de nature sexuelle est un autre exemple de cybercriminalité ayant des conséquences très lourdes. Par exemple, de jeunes victimes de ce type de cyberviolence peuvent être intimidées et harcelées sans relâche non seulement par le contrevenant, mais aussi par leurs pairs, ce qui peut engendrer des problèmes de santé mentale, comme l'angoisse et la dépression, ou même aboutir au suicide. En plus des répercussions à court terme de la cyberviolence de nature sexuelle, on en sait relativement peu sur les conséquences à long terme. Pour les victimes de tous âges, il peut être extrêmement traumatisant de savoir que les images de leur exploitation demeurent en circulation. Des victimes sont allées jusqu'à dire que le traumatisme persistant de savoir que ces images circulent est pire que la violence elle-même. Malgré tout, peu d'études ont été menées à ce jour sur ces types

[6] Statistique Canada, 2016, *Données sur les crimes haineux et les cybercrimes déclarés par la police*, *2014*; Crimes haineux déclarés par la police, selon l'infraction la plus grave, Canada, 2012.
[7] Statistique Canada, 2015, Statistiques sur les crimes déclarés par la police au Canada, 2015, *Juristat*, vol. 35, nº 1, nº de catalogue 85-002-X, ISSN 1209-6393.
[8] *Ibid*. et Cross, C., 2016, « I'm Anonymous, I'm a voice at the end of the phone : A Canadian case study into the benefits of providing telephone support to fraud victims », *Crime Prevention and Community Safety*, vol. 18, nº 3, p. 228-243.

particuliers de traumatismes et les meilleures façons d'aider ces victimes d'actes criminels.

Ce ne sont là que quelques exemples des répercussions négatives de la cybervictimisation pour la société et pour les victimes. Ils font ressortir l'importance d'aider et de soutenir les victimes afin de prévenir leur victimisation continue et d'atténuer les effets de la cybercriminalité.

Principales composantes de la lutte contre la cybervictimisation

Afin de bien évaluer, prendre en compte et combler les besoins des Canadiens et des Canadiennes qui sont devenues des victimes au moyen de la cybertechnologie, ou qui risquent de l'être, le BOFVAC recommande que le gouvernement du Canada envisage les principales composantes ci-dessous lorsqu'il élaborera ses stratégies ou ses politiques et qu'il donnera suite à nos recommandations.

Collecte de données et des statistiques

Recommandation nº 1 : Renforcer, régulariser et normaliser la collecte de données sur la cybervictimisation au Canada et envisager de lancer une nouvelle enquête nationale portant explicitement sur la cybercriminalité et la cybervictimisation et/ou une base de données de déclaration centralisée.

Il est difficile de mesurer et de quantifier la cybervictimisation. D'après les résultats du Programme de déclaration uniforme de la criminalité (DUC), selon Statistique Canada, 15 187 incidents de cybercriminalité ont été déclarés à la police en 2014[9], la fraude, la pornographie juvénile et les menaces figurant parmi les crimes graves les plus déclarés[10]. Toutefois, ces données ne représentent que la pointe de l'iceberg et constituent une sous-représentation de l'ampleur réelle de la cybervictimisation en

[9] Incidents déclarés aux services de police qui participent à la plus récente version du Programme de déclaration uniforme de la criminalité (DUC) (Statistique Canada), destiné à mesurer le taux de criminalité dans la société canadienne et les caractéristiques de celle-ci. Les données de la DUC représentent les crimes déclarés qui ont été corroborés par la police.
[10] *Ibid.*, p. 6.

raison d'un nombre de facteurs, par exemple la non-déclaration des données ou la non-déclaration à la police.

- **Non-déclaration par les victimes** – Les victimes peuvent être peu disposées à reconnaître qu'elles ont été victimisées parce qu'elles en ont honte (une victime peut avoir honte d'avoir fourni ses renseignements personnels à une personne qui avait l'intention de lui faire du tort) ou ne savent pas très bien ce qu'elles doivent faire (p. ex. si elles doivent ou non déclarer le crime et, le cas échéant, à qui)[11]. Elles peuvent aussi avoir peur qu'on ne les croie pas ou qu'on les blâme, une peur renforcée par le fait que d'autres victimes, après avoir relaté ce qu'elles ont vécu, se sont fait répondre « qu'elles n'auraient simplement pas dû naviguer sur Internet ». En outre, du temps peut s'être écoulé avant que les personnes s'aperçoivent qu'elles ont été victimisées et au moment où elles s'en rendent compte, elles peuvent décider qu'il n'est plus utile de déclarer l'incident à la police. S'il s'agit de jeunes, ceux-ci peuvent aussi craindre que le fait de déclarer l'incident entraîne un examen ou une surveillance plus intense de leurs activités en ligne.

- **Déclaration à d'autres autorités** – Même lorsque la cybervictimisation est déclarée, la déclaration ne passe pas toujours par un seul portail, comme la police, contrairement à ce qui peut se produire pour les renseignements relatifs à des crimes conventionnels[12]. Par exemple, une victime de fraude par carte de crédit pourrait ne déclarer l'incident qu'à sa banque et non à la police, ou un jeune qui vit de l'intimidation peut communiquer avec un site d'un réseau social ou un enseignant pour obtenir de l'aide.

En raison de ces facteurs et d'autres facteurs, dont le manque de collecte de données opportune sur l'éventail complet des types de cybervictimisation, l'ampleur réelle de la cybercriminalité et de la cybervictimisation au Canada est inconnue. Pour mieux comprendre les nuances et l'étendue du problème et être à même de mettre au point des réponses adaptées, le Canada a besoin d'indicateurs réguliers, systématiques et complets de la cybervictimisation. La collecte de données sur la victimisation au moyen d'enquêtes auprès de Canadiens et de Canadiennes, à une

[11] *Ibid.*, p. 5.
[12] Wall, D.S., 2005, The Internet as a Conduit for Criminals, dans A. Pattavina (dir.), *Information Technology and the Criminal Justice System*, p. 77-98, Thousand Oaks (Californie) : Sage (chapitre révisé en août 2015).

fréquence régulière, produirait un portrait plus clair, à jour et complet des problèmes qui sous-tendent les enjeux liés à la cybersécurité au Canada. Les renseignements serviraient non seulement à approfondir notre compréhension du vécu des cybervictimes afin de leur offrir des interventions adaptées, mais à renforcer aussi notre capacité à élaborer des politiques, des programmes et des lois fondés sur des données probantes, de façon plus générale.

Actuellement, en plus des données sur la cybercriminalité déclarées par la police collectées au moyen de la DUC, Statistique Canada recueille des données sur certains éléments de la cybervictimisation par l'entremise de l'Enquête canadienne sur l'utilisation d'Internet[13]. Ces données se rapportent à l'expérience des Canadiens et des Canadiennes quant à la mauvaise utilisation de renseignements personnels sur Internet et de demandes de renseignements financiers personnels reçues par courriel d'une source frauduleuse. Statistique Canada recueille aussi des données sur la victimisation basée sur Internet dans le cadre de l'Enquête sociale générale – Victimisation (l'ESG)[14]. Cette enquête demande aux Canadiens et aux Canadiennes de décrire leur vécu par rapport à plusieurs types de victimisation, notamment les incidents criminels déclarés à la police et ceux qui ne sont pas déclarés (c.-à-d. les incidents autodéclarés). Comme de nombreux actes criminels ne sont pas déclarés aux services policiers pour différentes raisons, les données sur la victimisation autodéclarée, comme celles fournies par l'ESG, représentent un complément essentiel aux statistiques du système de justice.

Une difficulté majeure tient au fait que l'Enquête sociale générale – Victimisation n'est répétée que tous les cinq ans[15], la plus récente enquête ayant été publiée en 2014. Par conséquent, nous n'avons pas accès à des statistiques à jour sur la cybervictimisation qui nous permettraient de suivre l'évolution de cette victimisation. Une autre difficulté tient au fait que ni l'Enquête canadienne sur l'utilisation de l'Internet ni l'Enquête sociale générale – Victimisation ne recueille de données sur une vaste gamme d'incidents de cybervictimisation. Par exemple, l'Enquête sociale générale – Victimisation de 2014 ne comportait des questions que

[13] L'Enquête canadienne sur l'utilisation de l'Internet est une enquête hybride qui mesure l'accès des ménages à Internet et les comportements en ligne des différents membres du ménage.
[14] La population cible est constituée de Canadiens et de Canadiennes âgés de 15 ans et plus. L'ESG sur la victimisation est la seule enquête nationale de la victimisation autodéclarée qui fournit des données pour les provinces et les territoires, y compris au moyen d'entretiens menés dans le nord du Canada.
[15] L'ESG porte sur six thèmes différents (soins donnés et reçus, familles, emploi du temps, identité sociale, dons, bénévolat et participation et victimisation), chaque thème étant répété en profondeur tous les cinq ans.

sur la cybervictimisation et le cyberharcèlement. Elle n'a pas repris les questions relatives à la cybervictimisation qui avaient été posées dans l'Enquête, pour la première fois, en 2009. L'Enquête de 2009 comportait des modules spéciaux qui avaient permis de recueillir des renseignements utiles auprès de Canadiens et de Canadiennes sur leur perception et leur vécu de la victimisation sur Internet par rapport à la cyberintimidation[16], le leurre d'enfants, la fraude bancaire par Internet, les problèmes éprouvés lors d'achats en ligne et le « hameçonnage » sous la forme de la réception de courriels frauduleux provenant d'une personne se faisant passer pour une organisation légitime qui demande des renseignements personnels. Le prochain cycle de l'Enquête sociale générale – Victimisation est prévu pour 2019 et le contenu est en voie d'élaboration. Cela pourrait offrir l'occasion d'ajouter du contenu pour combler les lacunes des données sur la cybervictimisation, par exemple des questions sur la cyberviolence de nature sexuelle, comme la pornographie de vengeance.

Comme l'Enquête sociale générale – Victimisation n'est répétée que tous les cinq ans et qu'elle ne constitue peut-être pas l'outil optimal pour évaluer la fréquence et les conséquences de la cybervictimisation, le BOFVAC est d'avis qu'une nouvelle enquête distincte sur la cybercriminalité et la cybervictimisation, élaborée en collaboration avec les provinces et les territoires, est justifiée. Une enquête autonome offrirait la possibilité de mettre régulièrement à jour son contenu afin de suivre l'évolution de la cybervictimisation. Elle permettrait aussi d'inclure des questions sur un éventail plus large de types de cybervictimisation, de même qu'un examen plus approfondi des enjeux, par exemple en insérant des questions sur l'issue de la cybervictimisation pour la victime (p. ex. si elle a eu accès à des services, les types de soutien reçu, le degré autodéclaré de préjudice vécu). Comme pour l'Enquête sociale générale – Victimisation, une éventuelle enquête de ce genre devrait s'en tenir aux incidents autodéclarés afin de bien saisir le vécu des victimes qui ne déclarent pas les incidents à la police.

À cette fin, le Canada pourrait s'employer à élaborer un système comme l'Australian Cybercrime Online Reporting Network (ACORN). ACORN est une base de données nationale conçue en collaboration avec la police, les entreprises, l'agence nationale

[16] L'ESG demandait aux répondants âgés de 15 ans et plus de décrire leur expérience personnelle de la cyberintimidation. Elle demandait aussi aux répondants âgés de 18 ans et plus ayant des enfants âgés de huit à 17 ans vivant dans leur ménage de décrire l'expérience des enfants par rapport à la cyberintimidation.

de la statistique de l'Australie et le gouvernement australien. Elle permet la déclaration et la mise en commun de renseignements sur une gamme complète des différents types de cybercriminalité, par exemple les fraudes en ligne, l'usurpation d'identité en ligne, la cyberintimidation, le sexting, le harcèlement en ligne et des illustrations de mauvais traitements ou d'exploitation sexuelle d'enfants en ligne. Les données peuvent être saisies par la police, des compagnies de cartes de crédit, des victimes de cybercriminalité, des entreprises qui ont été l'objet de cyberattaques ou de menaces et le département de la cybersécurité de l'Australie. L'agence nationale de la statistique de l'Australie peut consulter les données sans voir les renseignements personnels de façon à produire des rapports trimestriels sur le volume de la cybercriminalité et les principales tendances. Ainsi, le gouvernement dispose de renseignements de meilleure qualité sur la cybercriminalité et les menaces à la cybersécurité. Les policiers peuvent consulter les bases de données à des fins de renseignement pour enquêter sur des infractions ou cerner des tendances. Les compagnies de cartes de crédit et les banques peuvent utiliser les données à des fins d'assurance et pour recouvrer des pertes, et les entreprises peuvent consulter les données afin de mieux se protéger. ACORN a été présenté à l'assemblée annuelle de 2016 de l'Association canadienne des chefs de police comme étant une pratique prometteuse.

Au bout du compte, la disponibilité de statistiques fiables sur la cybervictimisation dépendra en grande partie de la disponibilité d'un ensemble complet de données sur la cybervictimisation provenant non seulement des déclarations par la police et des enquêtes sur la victimisation autodéclarée, mais aussi d'autres sources comme le Centre antifraude du Canada (l'agence centrale canadienne qui collecte des données et des renseignements criminels sur des questions comme la fraude par marketing de masse, l'escroquerie sur les droits payables à l'avance ainsi que la fraude et l'usurpation d'identité par Internet) et le Centre canadien de protection de l'enfance (qui exploite un service téléphonique national de dénonciation d'exploitation sexuelle d'enfants au Canada). Les mesures visant à uniformiser les définitions communes de différentes formes de cybercriminalité et de cybervictimisation dans les différents outils de collecte de données et à collaborer sur la création de mécanismes de saisie et d'échange de données plus harmonieux et intégrés, dans la mesure du possible, aideront aussi à produire un portrait plus fidèle de la cybercriminalisation au Canada.

Sensibilisation du public et formation

Recommandation nº 2 : Sensibiliser la population à la cybervictimisation et veiller à ce que le personnel du système de justice pénale reçoive une formation adéquate sur la cybervictimisation.

Les campagnes de sensibilisation et les programmes d'études peuvent grandement influer sur les perceptions sociales du comportement acceptable et être des outils efficaces pour aider la population à reconnaître la cybervictimisation. Les activités dans le cyberespace semblent défier la compréhension sociale de ce qui constitue ou non un comportement criminel[17]. Bien des gens ne sont pas conscients des préjudices liés à la victimisation criminelle dans le cyberespace ou ne considèrent pas que les préjudices qu'elle cause sont comparables à ceux d'autres formes de victimisation criminelle. Un vaste dialogue public est nécessaire pour :

- contrer le manque de sensibilisation à la cybercriminalité au sein de la population générale,
- renforcer la compréhension du fait qu'un crime commis en ligne est un crime,
- faire connaître les graves conséquences pour les victimes,
- encourager les victimes et d'autres personnes à déclarer les incidents,
- lutter contre la tendance actuelle consistant à blâmer la victime, que bien des victimes de victimisation sur Internet vivent,
- améliorer la culture numérique en matière de protection de la vie privée, de sécurité et quant à la façon dont nous interagissons les uns avec les autres en ligne.

Ce dialogue doit inclure *tous* les Canadiens et les Canadiennes et non seulement les jeunes et leurs parents.

Les efforts de sensibilisation devraient comporter des initiatives visant à augmenter la sensibilité au fait que la cybervictimisation touche un sexe plus que l'autre. Par

[17] *Ibid.*, p. 12.

exemple, bien que nous puissions tous être victimes de cyberviolence, la majorité de ces victimes, en particulier de la cyberviolence de nature sexuelle, sont des jeunes femmes et des filles. En 2012, la police a identifié 2 070 victimes de cybercriminalité violente, les femmes représentant 69 p. 100 de ces victimes, et 84 p. 100 des victimes d'infractions de nature sexuelle[18]. Le Projet national du YMCA Canada d'échange des connaissances sur la cyberviolence, un projet financé par Condition féminine Canada, est un exemple d'une initiative prometteuse qui augmente la sensibilisation au fait que la cybervictimisation touche un sexe plus que l'autre. Son objectif est de créer un univers numérique plus sûr pour les filles et les jeunes femmes. À l'appui de cet objectif, le Projet national a réalisé une étude d'évaluation des besoins mettant l'accent sur la détermination des enjeux propres à chacun des sexes liés à la cyberviolence. Le Projet national a communiqué les constatations issues de l'étude afin de réunir des appuis pour les stratégies qui ont été élaborées pour donner suite aux recommandations découlant de l'évaluation des besoins. L'objectif est de créer un changement systémique qui favorisera l'application d'une optique qui tient compte de la spécificité des sexes pour comprendre la cyberviolence et y réagir. L'évaluation et la compréhension des besoins des filles et des jeunes femmes en matière de sécurité en ligne au moyen d'initiatives comme le Projet national aideront à terme à créer de meilleurs appuis pour les victimes de la cyberviolence.

La sensibilisation générale est importante, mais il est également essentiel que les principaux intervenants du système de justice pénale soient formés pour répondre aux victimes d'une façon appropriée. Pour ce faire, ils doivent connaître les types de soutien dont une victime de la cybercriminalité peut avoir besoin, et fournir ces mesures de soutien d'une manière respectueuse et sans jugement.

Soutien pour les victimes

Recommandation nº 3 : Faire en sorte que des mesures de soutien axées sur la victime sont mises à la disposition des personnes qui ont vécu une cybervictimisation.

[18] Statistique Canada, 2014, Les cybercrimes déclarés par la police au Canada, 2012, *Juristat*, vol. 34, nº 1, nº de catalogue 85-002-X, ISSN 1209-6393

Les approches de lutte contre la cybercriminalité devraient accorder une attention particulière aux services de soutien axés sur la victime qui tiennent compte des caractéristiques particulières de la victimisation facilitée par la technologie. Le type de soutien dont les victimes de cybercriminalité peuvent avoir besoin peut varier de services très fondamentaux, par exemple la mise à disposition temporaire d'un téléphone ou d'un ordinateur pendant que les biens de la victime sont en la possession de la police aux fins d'une analyse judiciaire, ou des services plus cruciaux, par exemple la mise en place d'un engagement à garder la paix ou des services de counselling spécialisés pour les femmes qui ont vécu des menaces de violence en ligne. Des victimes peuvent aussi avoir besoin de conseils pour rétablir leur réputation financière ou personnelle, des avis sur la façon de se protéger d'une victimisation ultérieure[19], des aiguillages vers des services professionnels spécialisés adaptés pour aider les victimes de cybercriminalité et des renseignements sur leurs droits ainsi que sur l'enquête et le traitement de leur plainte[20].

Comme pour toutes les victimes, il est important de reconnaître que les victimes de cybercriminalité peuvent avoir besoin non seulement d'un soutien immédiat, mais aussi à plus long terme. Sous ce rapport, le Centre canadien de protection de l'enfance entreprend une enquête internationale auprès de la première génération des survivants de l'exploitation sexuelle en ligne afin de fournir un éclairage plus nuancé sur les répercussions à long terme pour les victimes de l'exploitation sexuelle d'enfants en ligne. Des recommandations sur la meilleure façon d'aider les victimes seront formulées. Des initiatives comme celle-ci, qui donnent une voix aux victimes, sont essentielles à notre compréhension, puisque ce sont les victimes elles-mêmes qui savent le mieux quels sont les types de soutien dont elles peuvent avoir besoin, et qui connaissent le mieux les éventuelles lacunes.

En plus de mesures de soutien concrètes, les mesures de soutien législatives et les droits protégés par la Constitution sont aussi importants dans une approche axée sur la victime. Bien que la situation et les besoins de chaque victime puissent varier, la *Charte canadienne des droits des victimes*[21] confère certains droits d'origine

[19] *Ibid.*, p. 5.
[20] *Ibid.*
[21] La *Charte canadienne des droits des victimes : Loi édictant la Charte canadienne des droits des victimes et modifiant certaines lois* a créé la *Loi visant la reconnaissance des droits des victimes* et modifié le *Code criminel*, la

législative à toutes les victimes d'actes criminels, une victime étant définie comme un « particulier qui a subi des dommages — matériels, corporels ou moraux — ou des pertes économiques par suite de la perpétration ou prétendue perpétration d'une infraction »[22]. Dorénavant, la lutte contre la cybercriminalité devra forcément garantir que ces victimes obtiennent justice et qu'elles puissent exercer les droits que leur confère la CCDV, en l'occurrence :

- **Droit à l'information –** Les victimes ont le droit de demander de l'information sur le système de justice pénale et les services et programmes qui leur sont offerts. Elles ont également le droit de demander des renseignements précis sur l'enquête, la poursuite, la détermination de la peine et la mise en liberté sous condition du ou des délinquants qui leur ont causé du tort.

- **Droit à la protection –** Les victimes ont droit à la prise en considération de leur vie privée et de leur sécurité à toutes les étapes du processus de justice pénale, ainsi qu'à la prise de mesures raisonnables et nécessaires pour les protéger contre les tentatives d'intimidation et les représailles. Elles ont aussi le droit de demander que leur identité ne soit pas dévoilée publiquement et que des mesures visant à faciliter leur témoignage leur soient offertes lorsqu'elles comparaissent comme témoins.

- **Droit à la participation –** Les victimes ont le droit d'exprimer leurs opinions sur des décisions qui auraient une incidence sur leurs droits en vertu de la CCDV et d'obtenir une prise en compte de ces opinions aux différentes étapes du processus judiciaire. Elles ont aussi le droit de présenter une déclaration de la victime à la cour ou au comité d'examen, et à la prise en compte de celle-ci.

Loi sur le système correctionnel et la mise en liberté sous condition, la *Loi sur la preuve au Canada* et la *Loi sur l'assurance-emploi*. Bien que la plupart des dispositions soient entrées en vigueur le 23 juillet 2015, d'autres l'ont été plus récemment, le 1er juin 2016.

[22] Comme l'alinéa 18(1)a) de la CCDV le précise, les droits s'appliquent à l'égard de la victime d'une infraction dans ses rapports avec le système de justice pénale pendant que l'infraction fait l'objet d'une enquête ou d'une poursuite; pendant que le délinquant est, à l'égard de l'infraction, régi par le processus correctionnel ou le processus de mise en liberté sous condition; pendant que l'accusé, dans le cas où il est déclaré inapte à subir son procès ou non responsable criminellement pour cause de troubles mentaux, relève, à l'égard de l'infraction, de la compétence du tribunal ou d'une commission d'examen.

- **Droit de demander un dédommagement –** Les victimes ont le droit que la cour examine la possibilité d'imposer une ordonnance de dédommagement au délinquant. En outre, toute victime en faveur de laquelle une ordonnance de dédommagement est rendue a le droit de la faire enregistrer au tribunal civil à titre de jugement exécutoire contre le délinquant en cas de défaut de paiement.

- **Droit de porter plainte -** Toute victime qui est d'avis qu'un ministère, une agence ou un organisme fédéral a violé un droit qui lui est conféré par la présente loi, ou l'en a privée, a le droit de déposer une plainte conformément au mécanisme d'examen des plaintes applicable. En outre, toute victime qui a épuisé les recours prévus par le mécanisme d'examen des plaintes et qui n'est pas satisfaite de la réponse peut déposer une plainte auprès de toute autorité compétente pour examiner les plaintes concernant l'entité fédérale en question, notamment le BOFVAC.

Partenariats multisectoriels

Recommandation nº 4 : Renforcer les partenariats de collaboration entre les secteurs.

Des études récentes donnent à penser que les solutions à la cybervictimisation nécessitent la collaboration de plusieurs partenaires : les jeunes et les jeunes chefs de file, les parents, les éducateurs, les chercheurs et les universitaires, les organismes d'application de la loi, l'industrie (p. ex., les fournisseurs de services Internet, les compagnies de téléphonie cellulaire, les sites de réseaux sociaux et de jeux en ligne, les développeurs de logiciel), les organisations non gouvernementales, les entreprises privées et les collectivités. Il faudra un effort global de tous les partenaires pour réussir à prévenir et à contrer la cybervictimisation.

Les organismes d'application de la loi devront aussi être souples dans leur approche puisque la cybercriminalité survient souvent hors des frontières provinciales/territoriales et nationales. Les données sur les incidents déclarés par la police révèlent que le territoire où l'infraction est déclarée n'est pas forcément celui où la victimisation est survenue. En conséquence, la coordination entre les corps policiers fédéraux et provinciaux/territoriaux s'impose même si les ressources et

les activités consacrées à la cybercriminalité peuvent varier d'un territoire à un autre[23].

La *Stratégie provinciale de protection des enfants contre l'exploitation et les agressions sexuelles sur Internet* de l'Ontario est un exemple d'une approche concertée à l'échelon provincial. La Police provinciale de l'Ontario, l'Association des chefs de police de l'Ontario, le Ministère de la Sécurité communautaire et des Services correctionnels et le ministère du Procureur général ont mis en œuvre une approche provinciale pluridisciplinaire pour lutter contre les crimes liés à l'exploitation d'enfants en ligne. L'approche garantit que les policiers et les procureurs de la Couronne sont formés aux circonstances particulières de l'enquête et de la poursuite de crimes sexuels dans le cyberespace et que des services de counselling spécialisés sont à la disposition des victimes. L'objectif consiste à s'attaquer efficacement au portrait complet des mauvais traitements et de l'exploitation sexuelle d'enfants – du début d'une enquête à l'arrestation et la gestion du délinquant jusqu'à la poursuite comme telle à la détermination de la peine, à l'identification et au soutien des victimes et à la prévention et à la sensibilisation[24].

Lois

Recommandation nº 5 : Veiller à ce que les Canadiens et les Canadiennes soient informés des lois en vigueur et combler les principales lacunes législatives concernant les images en ligne d'exploitation sexuelle et de mauvais traitements à l'égard d'enfants.

Les lois destinées à lutter contre la cybercriminalité doivent être régulièrement évaluées et mises à jour pour garantir que les recours juridiques efficaces existent et pour combler d'éventuelles lacunes. Vu la vulnérabilité des enfants et l'obligation du Canada de les protéger contre la violence, le BOFVAC est d'avis que la priorité devrait être accordée aux lacunes à combler par rapport à la protection des enfants

[23] *Ibid.*, p. 18.
[24] Police provinciale de l'Ontario (2016), *Backgrounder – Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet*, document consulté le 4 octobre à l'adresse suivante : http://www.opp.ca/index.php?id=115&entryid=571faa628f94ac3e7b0c6a45.

contre les formes d'exploitation sexuelle et de violence sexuelle en ligne et les images de mauvais traitements d'enfants en ligne.

Exploitation sexuelle d'enfants et violence sexuelle contre les enfants en ligne

De concert avec les gouvernements de quelques provinces, le gouvernement du Canada a promulgué des dispositions législatives prévoyant l'obligation de signaler le contenu pédopornographique possible. La déclaration obligatoire a pour objectif de faciliter le retrait de la pédopornographie de l'Internet, ce qui permet de réduire la circulation d'images d'exploitation sexuelle; d'aider les victimes; et d'identifier les auteurs de crimes contre des enfants. En outre, la *Loi sur la protection des Canadiens contre la cybercriminalité*, promulguée en mars 2015, permet d'intenter des poursuites pénales lorsque des images sexuelles sont diffusées sans consentement et lorsqu'il existe une attente raisonnable que les images soient gardées secrètes.

Bien qu'il existe des dispositions législatives pour lutter contre certaines formes d'exploitation sexuelle en ligne, des améliorations peuvent être nécessaires au fil du temps. La cybervictimisation de nature sexuelle peut prendre différentes formes, dont certaines peuvent ne pas être entièrement prises en compte dans le droit criminel. Les images qui illustrent la marchandisation sexuelle d'enfants, notamment des images ou des vidéos d'enfants mannequins sexualisés, sont un exemple. De telles images peuvent en venir à normaliser ou à promouvoir les préjudices contre les enfants tout en montrant des enfants qui sont en danger et pourtant, leurs auteurs peuvent échapper à des enquêtes ou à des poursuites criminelles. Dans son témoignage devant le Comité permanent de la condition féminine de la Chambre des communes sur la violence faite aux jeunes femmes et aux filles au Canada, la directrice générale du Centre canadien de protection de l'enfance a dit que « [b]ien que la définition canadienne actuelle de la pornographie juvénile soit assez vaste pour englober les cas les plus extrêmes d'enfants modèles sexualisés dans la définition du Code criminel, la majorité des images ne tombent pas sous le coup de la loi[25] ».

[25] Canada, Parlement, Chambre des communes, Comité permanent de la condition féminine, Témoignages, 42e législature, 1re session, numéro 023, le mercredi 28 septembre 2016. http://www.parl.gc.ca/content/hoc/Committee/421/FEWO/Evidence/EV8452214/FEWOEV23-F.PDF

En plus de combler les lacunes législatives, nous devons aussi veiller à ce que le personnel du système de justice pénale connaisse les lois en vigueur contre la cybercriminalité. Les témoignages recueillis au Comité sénatorial permanent de la condition féminine sur la violence faite aux jeunes femmes et aux filles au Canada[26] ont mis en lumière la variabilité de la sensibilisation et de la compétence, au sein du personnel du système de justice pénale, par rapport à la cybervictimisation. Des exemples ont été cités de jeunes femmes qui ont déclaré à la police que des images sexuelles les représentant étaient diffusées en ligne et qui se sont fait dire, à tort, qu'il n'y avait aucun recours juridique. Ce déphasage renforce l'importance de la sensibilisation publique et de la formation du personnel du système de justice pénale, de façon plus générale.

Images en ligne de violence physique à l'égard d'enfants

Un autre exemple d'un vide législatif se rapporte aux images en ligne de violence physique à l'égard d'enfants. Le *Code criminel* renferme des dispositions pour lutter contre la plupart des formes de pédopornographie, mais il ne renferme aucune disposition complémentaire qui interdit l'enregistrement et la diffusion ou la publication d'images de violence physique à l'égard d'enfants sur Internet ou qui oblige le retrait de ces images des réseaux de contenu Internet (p. ex., Facebook, Twitter, YouTube). Reconnaissant cette lacune, l'Association canadienne des chefs de police a adopté en août 2016 une résolution visant à lutter contre la prolifération de matériel en ligne illustrant de la violence physique à l'égard d'enfants. Étant donné que [TRADUCTION] « les images de violence physique à l'égard d'enfants violent la dignité, les droits et la vie privée des enfants victimisés et indiquent dans chaque cas qu'un enfant pourrait avoir désespérément besoin de protection », dans sa résolution, l'Association « presse le gouvernement du Canada de protéger les enfants en modifiant le *Code criminel* de façon à interdire la production et la publication d'images de violence physique à l'égard d'enfants et autorisant le retrait et la suppression de telles images d'Internet[27] ». Comme l'Association l'a souligné :

[26] Canada, Parlement, Chambre des communes, Comité permanent de la condition féminine, Témoignages, 42e législature, 1re session, numéro 022, le lundi 26 septembre 2016. http://www.parl.gc.ca/content/hoc/Committee/421/FEWO/Evidence/EV8437884/FEWOEV22-F.PDF

[27] Association canadienne des chefs de police, 2016, Résolutions adoptées à la 111e Conférence annuelle, consultées 18 août 2016 à l'adresse suivante : https://cacp.ca/resolution.html?asst_id=1199.

> *Les forces de l'ordre sont empêchées de faire enquête sur de telles affaires ainsi que leur mandat l'exigerait, du fait que, comme cela s'est vu souvent, la technologie Internet et son utilité sociale ont progressé plus rapidement que la loi. La présence sur Internet d'images de violence physique à l'égard d'enfants est l'équivalent d'une affiche matérielle ou d'une annonce télévisée montrant des violences à l'égard d'enfants. La communauté serait d'accord que de telles images sont odieuses et contraires aux normes de tolérance de la collectivité. Cependant, de telles images sont aujourd'hui permises en ligne même si la portée d'Internet est beaucoup plus grande que celle de toute annonce ou affiche matérielle*[28]*.*

Le BOFVAC est lui aussi préoccupé par le manque de lois pour lutter contre les illustrations en ligne de violence physique à l'égard d'enfants. Cela fait en sorte qu'il n'existe aucun mécanisme pour permettre d'enquête sur ceux qui victimisent des personnes en publiant en ligne des images de violence physique à l'égard d'enfants, et de les arrêter, afin de faciliter la protection de ces victimes contre la poursuite des préjudices ou de forcer le retrait des images d'Internet. Actuellement, il revient aux fournisseurs de contenu de déterminer s'ils doivent prendre des mesures et la nature de ces mesures (p. ex., retirer les images, bloquer l'utilisateur) en accord avec leurs politiques internes. En outre, les fournisseurs de contenu ne sont pas tenus de fournir les renseignements nécessaires aux forces de l'ordre. Comme pour la pédopornographie, des dispositions législatives doivent prévenir les préjudices causés à l'enfant et à la population par la publication et la diffusion d'illustrations de violence physique à l'égard d'enfants. Le fait que ces images soient enregistrées et distribuées sur Internet victimise de nouveau les enfants victimes, peuvent traumatiser ceux qui les voient et en venir à normaliser – ou pire, à promouvoir la violence envers des enfants. Le BOFVAC est donc d'avis que des modifications législatives sont nécessaires pour protéger les victimes et le grand public.

[28] *Ibid.*, ACCP, résolution 2016-02, Images de violence physique à l'égard d'enfants.

Conclusion

Dans le cadre de l'élaboration d'une réponse aux problèmes auxquels nous sommes confrontés en matière de cybersécurité, il est essentiel que le Canada tienne compte des victimes. Comment pouvons-nous prévenir le plus efficacement possible la victimisation? Quelles sont les conséquences de ces crimes pour les victimes à court, moyen et long terme? Que vivront les victimes dans le système de justice pénale et comment pouvons-nous répondre le mieux à leurs besoins et à leurs préoccupations?

Des données et des études devraient sous-tendre et guider une réponse efficace. La collecte et l'analyse régulières de données sont donc des composantes importantes. Une réponse efficace nécessitera aussi une conversation qui mobilisera *tous* les Canadiens et les Canadiennes afin de changer les attitudes de la société et de faire connaître non seulement le risque de victimisation, mais aussi les besoins des victimes dans le sillage d'un crime. La connaissance va de pair avec la formation et la sensibilisation des personnes qui travaillent auprès des victimes dans le système de justice pénale afin qu'elles comprennent mieux les besoins propres aux victimes de la cybercriminalité et en tiennent mieux compte. La prévention est l'objectif, mais des réponses axées sur la victime doivent être disponibles pour contrer les préjudices causés aux personnes qui ont été touchées par les nombreux types différents de cybervictimisation. Ces réponses doivent être élaborées et mises en place dans tous les secteurs. Les victimes, y compris les jeunes victimes, et les organismes de services aux victimes possèdent une expertise particulière et importante qu'ils peuvent mettre à profit dans la conversation et leur apport devrait aider à guider la prise de décisions concernant les politiques, les programmes et les lois. Enfin, les lois en vigueur doivent refléter la réalité d'un environnement technologique qui évolue rapidement et des besoins et des préoccupations propres aux victimes d'actes criminels. Nous devons veiller à ce que les lois du Canada protègent les enfants et envoient un message clair que toute forme de violence ou de marchandisation sexuelle à l'égard d'enfants est simplement inacceptable.

Pour conclure, le BOFVAC soumet respectueusement ses recommandations au gouvernement du Canada et est ravi d'avoir l'occasion de participer à la poursuite de cet important dialogue.

Résumé des recommandations

- **Recommandation nº 1 :** Renforcer, régulariser et normaliser la collecte de données sur la cybervictimisation au Canada et envisager de lancer une nouvelle enquête nationale portant explicitement sur la cybercriminalité et la cybervictimisation et(ou) une base de données de déclaration centralisée.

- **Recommandation nº 2 :** Sensibiliser la population à la cybervictimisation et veiller à ce que le personnel du système de justice pénale reçoive une formation adéquate sur la cybervictimisation.

- **Recommandation nº 3 :** Faire en sorte que des mesures de soutien axées sur la victime sont mises à la disposition des personnes qui ont vécu une cybervictimisation.

- **Recommandation nº 4 :** Renforcer les partenariats de collaboration entre les secteurs.

- **Recommandation nº 5 :** Veiller à ce que les Canadiens et les Canadiennes soient informés des lois en vigueur et combler les principales lacunes législatives concernant les images en ligne d'exploitation sexuelle et de mauvais traitements à l'égard d'enfants.

Sources

Canada, Parlement, Chambre des communes, Comité permanent de la condition féminine, Témoignages, 42e législature, 1re session, numéro 023, le mercredi 28 septembre 2016. http://www.parl.gc.ca/content/hoc/Committee/421/FEWO/Evidence/EV8452214/FEWOEV23-F.PDF

Canada, Parlement, Chambre des communes, Comité permanent de la condition féminine, Témoignages, 42e législature, 1re session, numéro 022, le lundi 26 septembre. http://www.parl.gc.ca/content/hoc/Committee/421/FEWO/Evidence/EV8437884/FEWOEV22-F.PDF

Canada. Statistique Canada. (2016). Données sur les crimes haineux et les cybercrimes déclarés par la police, 2014 : Crimes haineux déclarés par la police, selon l'infraction la plus grave, Canada, 2014.

Canada. Statistique Canada. (2015). Les cybercrimes déclarés par la police au Canada, 2014, *Juristat*, vol. 35, no 1, no de catalogue. ISSN 1209-6393.

Canada. Statistique Canada. (2014). Les cybercrimes déclarés par la police au Canada, 2012, *Juristat*, vol. 34, no 1, no de catalogue 85-002-X. ISSN 1209-6393.

Canada. Statistique Canada. (2014). Données sur les crimes haineux et les cybercrimes déclarés par la police, 2014.

Association canadienne des chefs de police, 2016, Résolutions adoptées à la 111e Conférence annuelle, consulté le 18 août 2016 à l'adresse suivante : https://cacp.ca/resolution.html?asst_id=1199.

Cross, C. (2016). I'm Anonymous, I'm a voice at the end of the phone : A Canadian case study into the benefits of providing telephone support to fraud victims. *Crime Prevention and Community Safety, 18*(3), p. 228-243.

Gelder, Gingras & Associates. (2016). *Final Report : Environmental Scan and Gap Analysis – Online and Technology Facilitated Child Sexual Exploitation*. Ottawa : Sécurité publique Canada.

Hinduja, S. et Patchin, J.W. (2014). *Cyberbullying Identification, Prevention and Response*. Cyberbullying Research Center, consulté le 22 septembre 2016 à l'adresse

suivante : http://cyberbullying.org/Cyberbullying-Identification-Prevention-Response.pdf.

International Centre for Criminal Law Reform and Criminal Justice Policy. (2011). *Responding to Victims of Identity Crime : A Manual for Law Enforcement Agents, Prosecutors and Policy-makers*, consulté le 4 octobre 2016 à l'adresse suivante : http://icclr.law.ubc.ca/sites/icclr.law.ubc.ca/files/publications/pdfs/00%20Victims%20of%20Identity%20Crime%20Manual.pdf

Kiriakidis, S., et Kavoura, A. (2010). Cyberbullying : A review of the literature on harassment through the internet and other electronic means. *Family and Community Health*, *33*(2), 82-93.

Police provinciale de l'Ontario. (2016). *Backgrounder – Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet*, consulté le 4 octobre 2016 à l'adresse suivante : http://www.opp.ca/index.php?id=115&entryid=571faa628f94ac3e7b0c6a45.

Gendarmerie royale du Canada, 2016, *Intimidation et Cyberintimidation*, consulté le 7 octobre 2016 à l'adresse suivante : http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-fra.htm.

Wall, D.S. (2005). The Internet as a Conduit for Criminals. In A. Pattavina, (éd.), *Information Technology and the Criminal Justice System* (p. 77-98). Thousand Oaks (Californie) : Sage (chapitre révisé, mars 2010).