



Sommaire de recherche sur la violence familiale et le droit de la famille

La violence facilitée
par la technologie :
une introduction

Numéro 14 | *Mars, 2022*



ALLIANCE DES CENTRES
DE RECHERCHE CANADIENS
SUR LA VIOLENCE BASÉE SUR LE GENRE

Le présent sommaire a été conçu par RESOLVE Manitoba (Research and Education for Solutions to Violence and Abuse), membre de l'Alliance des centres de recherche canadiens sur la violence basée sur le genre.

RESOLVE Manitoba est établi à l'Université du Manitoba, à Winnipeg, au Manitoba, au Canada, sur les terres ancestrales des peuples Anichinabés, Cris, Oji-Cris, Dakota et Déné et sur la terre natale de la Nation Métis.

Citation suggérée

Hoffart, R. & Kardashevskaya, M. (2022). La violence facilitée par la technologie : une introduction. Sommaire de recherche sur la violence familiale et le droit de la famille (14). Winnipeg, Manitoba: RESOLVE (Research and Education for Solutions to Violence and Abuse)

Édition

Diana Corredor, coordonnatrice des communications au Centre de recherche et d'éducation sur la violence contre les femmes et les enfants, & Patricia Karacsony, spécialiste des communications numériques, RESOLVE

Traduction

Sylvie Rodrigue

Partager vos commentaires sur ce sommaire

Cliquez sur le lien ci-dessous pour faire part de vos commentaires sur ce sommaire ou de vos suggestions sur des ressources futures :

https://uwo.eu.qualtrics.com/jfe/form/SV_bayzVPBefHsfER8

Nous joinder

Écrivez-nous pour recevoir de l'information sur nos futurs ressources et webinaires : RESOLVE@umanitoba.ca

Le présent sommaire est fondé sur la présentation de Jane Bailey et Suzie Dunn, « La violence facilitée par la technologie : une introduction » [en anglais], qui a été présentée le 24 novembre 2021 par RESOLVE, au Manitoba. Le webinaire peut être consulté au lien suivant : <https://www.youtube.com/watch?v=GXL0qNfIWI>



Public Health
Agency of Canada

Agence de la santé
publique du Canada

La violence facilitée par la technologie : une introduction

Introduction

Le monde connaît une plus grande accessibilité à des technologies comme l'Internet, les téléphones intelligents, divers logiciels et applications et l'intelligence artificielle (IA), et les médias sociaux sont omniprésents. De plus, les niveaux d'utilisation et de dépendance à l'égard de ces technologies ont augmenté.

La technologie offre de nouvelles façons de lutter contre la violence fondée sur le sexe, par exemple au moyen de campagnes dans les médias sociaux qui ciblent divers publics ou d'applications pour téléphones intelligents qui peuvent aider les survivantes de violence familiale à accéder à des services de soutien (Emezue, 2020). Toutefois, ces nouvelles technologies posent également des défis importants lorsqu'il s'agit de lutter contre la violence fondée sur le sexe. Ainsi, en 2014, la BC Society of Transition Houses (BCSTH) a mené un sondage auprès des fournisseurs de services au sujet de l'intersection de la violence et de la technologie, et a constaté que :

- 98 % des fournisseurs de services avaient travaillé avec des femmes et des filles qui avaient été menacées par la technologie
- 72 % soutenaient des femmes et des filles dont le courriel et les comptes de médias sociaux avaient été piratés
- 69 % appuyaient des femmes et des filles dont l'agresseur s'était fait passer pour elles dans un espace en ligne (p. ex., page de médias sociaux, site de rencontre)
- 89 % des fournisseurs de services ont exprimé le besoin d'obtenir plus de renseignements sur la violence facilitée par la technologie

Ce court sommaire explore la question de la violence facilitée par la technologie. Il se fonde sur le webinaire *Tech-Facilitated Violence : An Introduction* (Violence facilitée par la technologie : une introduction), animé par RESOLVE à l'Université du Manitoba avec les conférencières principales Jane Bailey (Université d'Ottawa, The eQuality Project) et Suzie Dunn (Université Dalhousie, The eQuality Project). Ce sommaire fournit des termes et des définitions de base, donne un aperçu de la violence facilitée par la technologie (VFT), traite de la violence fondée sur le sexe facilitée par la technologie (VFSFT), examine la question de la violence familiale facilitée par la technologie et fournit des conseils pratiques pour la planification de la sécurité, ainsi qu'une liste de ressources utiles.

Termes et définitions

Il existe de nombreuses formes de violence facilitée par la technologie qui impliquent de multiples formes de technologie et une myriade de stratégies de maltraitance. Dunn (2020) regroupe la violence facilitée par la technologie en quatre catégories : harcèlement, abus sexuel fondé sur l'image, atteintes à la vie privée et usurpation d'identité :

1. Harcèlement : comprend toute forme de communication numérique non désirée. Il s'agit de la forme de violence facilitée par la technologie la plus courante et la mieux connue, et elle peut prendre n'importe laquelle des formes suivantes.

- **Messages non désirés :** peuvent comprendre des messages préjudiciables d'un partenaire actuel ou ancien, des communications non désirées de la part de connaissances ou la réception d'images sexuelles explicites non sollicitées qui ont été envoyées dans l'intention de déranger le ou la destinataire et de lui causer du tort.
- **Harcèlement en réseau :** fait intervenir des groupes de personnes (réseaux) qui se sont réunis pour cibler une seule personne ou un seul type de personne dans l'intention de lui causer du tort.
- **Diffamation :** se produit lorsque des personnes ou des groupes partagent en ligne de faux renseignements qui nuisent à la réputation d'une personne ou d'un groupe de personnes. La diffamation peut aussi être liée à de faux sites Web et à l'usurpation d'identité, qui sont tous deux examinés plus en détail ci-dessous.
- **Menaces :** sont une autre forme communément reconnue de violence facilitée par la technologie qui peut comprendre des menaces de mort et des menaces de violence sexuelle, qui sont normalisées dans l'espace numérique. Dans bien des cas, ces menaces visent les personnes en fonction de leur situation sociale et visent souvent les femmes et les membres des communautés 2SLGBTQ+.
- **Discours haineux :** est une communication désobligeante en ligne qui vise une personne ou un groupe en raison de caractéristiques liées à la race, à la classe sociale, au genre, à l'orientation sexuelle ou à d'autres catégories semblables. Dans les espaces en ligne, le discours haineux est souvent dirigé vers les femmes et les membres de groupes racialisés.

2. Abus sexuel fondé sur l'image : implique la distribution d'images intimes. Cette forme d'abus est relativement courante et peut prendre de nombreuses formes différentes, y compris ce qu'on appelle souvent la distribution non consensuelle d'images intimes.

- **Voyeurisme/« creepshots » :** se produit lorsqu'une personne utilise un appareil caché (p. ex., caméra, enregistreur vidéo) pour prendre des images ou des vidéos secrètes d'une personne dans des endroits où elle peut raisonnablement s'attendre à ce que sa vie privée soit protégée.
- **Diffusion en direct et consignation des voies de fait :** comprend l'enregistrement, la documentation numérique et la distribution des voies de fait et des agressions sexuelles. Il s'agit d'une stratégie visant à amplifier la violence et à créer un autre niveau de violence.
- **Sextortion :** se produit lorsqu'une personne utilise l'image intime d'une autre personne (consensuelle ou non consensuelle) pour forcer sa victime à rester dans une situation non désirée. Elle peut survenir dans le contexte de relations violentes ou de la traite de personnes.
- **Hypertrucage (« deepfakes ») :** consiste à utiliser la technologie de l'intelligence artificielle pour permuter les visages des gens dans des vidéos ou d'autres images. Il s'agit souvent d'insérer l'image d'une personne dans des vidéos à caractère sexuel sans son consentement. Il s'agit d'une forme technologiquement plus avancée d'abus fondé sur l'image.

- 3. Atteinte à la vie privée :** est une forme de violence technique où des personnes divulguent des renseignements personnels sur une autre personne en ligne sans son consentement.
- **Divulgarion publique de renseignements personnels :** est la publication en ligne de renseignements privés et/ou de photos embarrassantes sans le consentement d'une personne.
 - **Doxing (divulgarion des données personnelles) :** signifie trouver les renseignements personnels d'une personne (p. ex., adresse personnelle, numéro de téléphone) et les publier en ligne sans son consentement. Ces renseignements sont ensuite utilisés pour intimider la victime.
 - **Traque et surveillance :** peuvent comprendre des formes complexes de technologie (logiciel traqueur) qui sont installées sur les appareils de la victime et utilisées pour surveiller ses activités. La traque et la surveillance peuvent également faire appel à des applications de base comme Find My iPhone. Cette forme de violence peut aussi être perpétrée dans les cas où l'auteur de violence exige d'avoir accès aux appareils de sa victime.

4. Usurpation d'identité : est l'utilisation de la technologie pour nuire à la réputation de la victime en se faisant passer pour elle sur les plateformes de médias sociaux, dans les profils de rencontre, sur des sites Web ou d'autres espaces en ligne, ce qui peut être particulièrement préjudiciable en raison de l'importance et de l'impact croissants de la réputation des gens en ligne.

- **Faux sites Web :** une personne crée un faux site Web au sujet de ses victimes dans le but de nuire à leur réputation. Il peut s'agir d'afficher de l'information personnelle, privée, nuisible ou embarrassante sur la victime et de répandre des mensonges.
- **Faux profils de rencontre :** une personne crée un faux profil de rencontre pour sa victime sans son consentement et indique faussement que cette personne est disponible pour des activités sexuelles ou des fantasmes de viol.
- **Mystification (« spoofing ») :** est l'envoi de « faux » messages textes ou de courriels de sorte qu'ils semblent provenir des comptes de téléphone ou de courriel de la victime, alors que ce n'est pas le cas. Une personne peut agir ainsi pour mettre sa victime dans le pétrin pour quelque chose qu'elle n'a pas dit ou fait. Il est difficile de prouver qu'il y a eu mystification, car la communication semble provenir des comptes de la victime.

La violence fondée sur le sexe facilitée par la technologie

La violence fondée sur le sexe (VFS) est une violence dirigée contre une personne ou un groupe de personnes en fonction de leur identité de genre, de leur expression de genre ou de leur genre perçu. Elle peut toucher des personnes de n'importe quelle identité de genre; toutefois, la violence fondée sur le sexe cible souvent les femmes, les filles et les personnes de diverses identités de genre, en particulier celles issues des groupes marginalisés (Gouvernement du Canada, 2021). La VFS est un problème social important qui a traditionnellement été compris dans le contexte des interactions hors ligne. Toutefois, plus récemment, avec l'accessibilité des technologies numériques et la centralité croissante des interactions en ligne, de nouvelles formes de violence sont facilitées par la technologie. La violence fondée sur le sexe facilitée par la technologie (VFSFT) peut être comprise comme étant une composante du continuum plus vaste de la violence fondée sur le sexe (Khoo, 2021).

Les données de l'Enquête sociale générale (ESG) de 2014 illustrent la nature sexospécifique du cyberharcèlement et de la cyberintimidation dans la société canadienne. Un peu moins d'un cinquième (17 %) des jeunes Canadien.ne.s de 15 à 29 ans ont déclaré avoir été victimes de cyberintimidation ou de cyberharcèlement. Les jeunes (en particulier ceux qui ont déjà été victimes de violence ou de discrimination), les personnes de diverses identités de genre et les femmes étaient plus susceptibles de déclarer avoir vécu ces formes de violence facilitée par la technologie (Burlock et Hudon, 2018; Hango, 2016). Les filles et les jeunes femmes activistes qui parlent de l'égalité des sexes et d'autres questions de justice sociale sont susceptibles de subir de la violence facilitée par la technologie à un très jeune âge, ce qui peut avoir une incidence négative sur le développement social global et la justice de genre (Bailey et Dunn, 2021).

La VFSFT est un terme utilisé pour désigner une « action d'une ou de plusieurs personnes qui cause du tort à autrui en raison de leur identité sexuelle ou de genre, ou en appliquant des normes de genre préjudiciables » et qui est « effectuée au moyen d'Internet ou de la technologie mobile et comprend la traque, l'intimidation, le harcèlement sexuel, la diffamation, le discours haineux et l'exploitation » [traduction libre] (Hinson et coll., 2018, p. 1). La VFSFT a aussi été qualifiée de cyberintimidation, de trollage, d'abus en ligne, de cyberviolence, de harcèlement numérique, de contrôle coercitif facilité par la technologie, de violence symbolique et de violence représentative (Bailey et Dunn, 2021). La VFSFT est un problème social sexospécifique étant donné que les femmes, les filles, les personnes de diverses identités de genre et les personnes de genre non conforme sont souvent visées. Cette forme de violence recoupe également d'autres formes de discrimination, y compris celles liées à la race, à la classe sociale, au handicap et à l'orientation sexuelle (Dunn, 2021).

Des technologies comme les traceurs du système de positionnement global (GPS), les plateformes de médias sociaux, les applications pour téléphones intelligents et les dispositifs de l'Internet des objets (p. ex., les serrures intelligentes, les haut-parleurs intelligents) ont

été utilisées dans la perpétration de la VFSFT (Slupska et Tanczer, 2021). Il y a aussi de nouvelles formes de violence qui sont apparues avec l'accessibilité et l'importance accrues des technologies. Le doxing, l'usurpation d'identité, l'hypertrucage, le voyeurisme et la mystification ne sont que quelques exemples de la violence facilitée par la technologie qui ont été utilisés pour intimider, menacer, miner, harceler et contrôler les victimes (Bailey et Dunn, 2021; Dunn, 2020).

La VFSFT est également un problème intersectionnel qui a des répercussions négatives disproportionnées sur les femmes qui occupent des postes de direction (p. ex., politiciennes, activistes, défenseuses des droits de la personne), ainsi que sur les femmes des communautés noires, autochtones et d'autres communautés racialisées, celles qui sont des victimes/survivantes de la VC, les membres des communautés 2SLGBTQ+, les femmes handicapées et les jeunes.

Impacts de la violence fondée sur le sexe facilitée par la technologie

La VFSFT peut avoir des effets dévastateurs sur les victimes/survivantes, en particulier en ce qui concerne leur statut social, car elle crée un dossier numérique permanent qui peut être diffusé à l'échelle mondiale et n'est pas facile à effacer (Šimonović, 2018). Elle peut nuire à la réputation, entraîner une perception négative de soi, l'humiliation dans la communauté, des problèmes de santé mentale (y compris le TSPT, les idées suicidaires, l'anxiété, etc.) et des difficultés financières (p. ex., la perte d'un emploi). La VFSFT et ses effets négatifs ne se limitent pas au monde en ligne. Il peut s'agir d'un prolongement de la violence hors ligne que les survivantes vivent, et ses effets peuvent imprégner tous les aspects de leur vie (Bailey et Dunn, 2021; Dunn, 2020).

À un niveau systémique, la VFSFT réduit au silence les femmes et d'autres groupes marginalisés en réduisant leur « participation aux espaces numériques et leur rôle de leadership » [traduction libre], ce qui exacerbe l'impuissance sociale, économique et politique des femmes, des filles et d'autres groupes marginalisés (Dunn, 2020, p. 22). Khoo (2021) soutient que cela peut avoir un effet désastreux sur la qualité de la démocratie.

En dépit d'une sensibilisation croissante aux répercussions de la VFSFT, il y a un besoin qui persiste de comprendre de façon nuancée les conséquences négatives pour les survivantes et d'élaborer des solutions possibles à ce problème. La violence qui se produit dans les espaces numériques est souvent mal comprise et, dans certains cas, elle peut être perçue comme mineure ou insignifiante. Par conséquent, les autorités risquent de ne pas reconnaître le problème et/ou de ne pas prendre de mesures à cet égard. Dans de nombreux cas, la solution proposée pour la violence facilitée par la technologie consiste pour la victime/survivante à limiter son activité en ligne, à se censurer ou à se déconnecter de la technologie (Dunn, 2021). Cependant, l'autocensure et la déconnexion ne sont pas des solutions viables en raison de l'importance de la présence en ligne individuelle dans le monde d'aujourd'hui. De plus, dans certains cas, les expériences des victimes/survivantes ne sont pas prises en compte dans le droit pénal existant (Khoo, 2021).

Trouver une voie à suivre

Pour s'attaquer de façon significative à la VFSFT et soutenir les survivantes, il faut une approche à plusieurs volets qui pourrait comprendre des solutions juridiques, éducatives et technologiques. De nombreuses plateformes numériques (p. ex., Facebook, Twitter, YouTube) ont élaboré des politiques communautaires qui interdisent les discours haineux, l'incitation à la violence, la pornographie et la nudité. Bon nombre de ces plateformes sont également dotées d'outils qui permettent de vérifier les faits, et de signaler et modérer le contenu nuisible. Ces politiques et ces outils ne se sont toutefois pas révélés particulièrement efficaces pour diverses raisons. Par exemple, dans certains cas, le modèle d'affaires de ces entreprises fait en sorte qu'il est rentable de laisser du contenu nuisible, ce qui les rend réticentes à mettre en œuvre des stratégies pour lutter de façon significative contre la VFSFT (Khoo, 2021). Khoo (2021) soutient qu'il devrait y avoir des changements de politique au Canada pour lutter contre la VFSFT sur ces plateformes, comme l'établissement d'un organisme de réglementation spécialisé centralisé pour la VFSFT et un processus qui permet le retrait rapide et efficace de certains contenus nuisibles sans ordonnance du tribunal. Les solutions stratégiques, cependant, doivent intégrer une analyse intersectionnelle et mettre l'accent sur l'égalité réelle afin de s'assurer qu'elles ne finissent pas

par nuire aux personnes mêmes qu'elles sont censées servir et appuyer. Khoo (2021) fait également valoir qu'il faut plus de financement pour appuyer la recherche visant à comprendre les complexités de la VFSFT et pour élaborer des services améliorés pour les victimes/survivantes.

Violence familiale facilitée par la technologie

Comme il a été mentionné précédemment, la VFSFT est souvent utilisée dans des relations de violence, les auteurs de violence utilisant une multitude d'outils pour contrôler leurs victimes (Laxton, 2014). La dynamique de pouvoir et de contrôle associée à la VC est particulièrement importante lorsqu'elle est réalisée au moyen de la technologie, car les auteurs de violence sont en mesure de surveiller et de contrôler les actions de leurs victimes, ce qui crée un sentiment d'omniprésence (Bailey et Dunn, 2021). La violence familiale facilitée par la technologie (VCFT) peut être une stratégie particulièrement débilatante en raison de sa nature constante et envahissante.

La recherche (Freed et coll., 2017; Borrajo et coll., 2015) a permis d'identifier plusieurs formes de VCFT couramment observées dans les relations violentes, notamment :

- la traque et le harcèlement en ligne
- l'envoi d'insultes et de menaces sur les plateformes de médias sociaux, par courriel et par message texte
- le partage de renseignements privés ou embarrassants sur la victime dans des espaces en ligne
- l'utilisation de technologies (p. ex., Find My iPhone, logiciel traqueur) pour surveiller les appareils et les activités en ligne de la victime

Certains aspects de la VCFT placent les auteurs de violence dans des positions particulièrement puissantes. Par exemple, dans bien des cas, l'auteur de violence a accès aux appareils et aux comptes en ligne de la victime. Les auteurs de violence emploient souvent des stratégies coercitives pour faire pression sur leurs victimes afin qu'elles communiquent cette information. Grâce à cette accessibilité, il peut facilement apporter des changements aux comptes de médias sociaux de la victime, installer un logiciel de surveillance ou manipuler ses renseignements d'une autre façon. Les auteurs de violence peuvent être en mesure de découvrir les mots de passe des appareils et des médias sociaux de la victime parce qu'ils connaissent ses circonstances de vie, ce qui leur permet de répondre correctement aux questions de sécurité (Dunn, 2020).

Les complexités de la violence facilitée par la technologie posent des défis importants au processus de planification de la sécurité. Par conséquent, les stratégies de planification de la sécurité doivent tenir compte de la dynamique particulière de pouvoir et de contrôle qui existe dans le contexte de la VFT. L'éducation et la sensibilisation à cet enjeu, combinées à une responsabilité et responsabilisation accrues des entreprises et de la police, ainsi qu'à l'amélioration de la littératie technologique et de la sécurité en ligne sont des points de départ importants pour s'attaquer au problème.

Planification de la sécurité – Violence familiale facilitée par la technologie

Les conseils suivants en matière de planification de la sécurité ont été adaptés de ressources produites par la British Columbia Society of Transition Houses (2022) et HackBlossom (2022).

- 1. Recherchez des tendances.** Pensez aux façons dont la technologie peut être utilisée pour harceler, surveiller ou traquer. Identifiez les modèles de violence et déterminez les formes de technologie utilisées pour commettre la violence, et utilisez cette information pour élaborer un plan de sécurité. Documentez les incidents et signalez-les aux autorités.
- 2. Pensez à utiliser un appareil plus sécuritaire.** Si vous pensez que quelqu'un surveille votre ordinateur, votre téléphone intelligent ou votre tablette, envisagez d'utiliser un appareil différent auquel l'agresseur n'a pas eu accès physiquement ou à distance.
- 3. Changez vos mots de passe et vos noms d'utilisateur.** Passez en revue les paramètres de confidentialité de vos appareils. Assurez-vous que l'accès d'un appareil à l'autre est désactivé et que d'autres comptes ne sont pas liés au vôtre. Utilisez des mots de passe robustes pour réduire les risques de piratage de vos comptes. Pensez à utiliser la vérification en deux étapes pour vos comptes.
- 4. Surveillez les niveaux d'utilisation des données.** Des pics dans l'utilisation des données peuvent indiquer qu'un logiciel de surveillance est utilisé.
- 5. Protégez votre emplacement.** Passez en revue les paramètres, les applications et les comptes de votre téléphone intelligent pour déterminer si le partage de votre emplacement est activé. Communiquez avec votre fournisseur de services sans fil et les services d'assistance routière ou de conduite sécuritaire pour déterminer si la localisation est activée dans vos comptes.
- 6. Protégez votre adresse et limitez les informations que vous donnez à votre sujet.** Limitez le nombre de personnes avec lesquelles vous partagez vos renseignements personnels. Évitez de partager vos renseignements personnels et vos coordonnées sur les plateformes de médias sociaux.
- 7. Obtenez plus d'informations.** Communiquez avec les centres de ressources, les refuges et les organismes d'application de la loi à l'échelle locale pour obtenir de l'aide. Des renseignements supplémentaires et des ressources sur la planification de la sécurité se trouvent dans la section *Ressources* du présent document.

Violence familiale facilitée par la technologie et questions relatives aux tribunaux de la famille

Les modifications apportées récemment à la *Loi sur le divorce* comprennent une définition de la violence familiale qui est exhaustive et englobe un large éventail de comportements violents, y compris la traque et le harcèlement. Les appels, les courriels et les textos répétés à une victime; la surveillance des activités d'une victime au moyen d'applications ou de logiciels spécialisés (p. ex., logiciel traqueur); et la surveillance de la victime au moyen des plateformes de médias sociaux sont des exemples de traque et de harcèlement facilités par l'utilisation de la technologie (Ministère de la Justice, 2022). La VCFT est une question importante dans le système des tribunaux de la famille et elle a des répercussions importantes pour les survivantes et leurs enfants. Un examen récent des affaires de droit de la famille a révélé que la technologie (c.-à-d. les courriels, les textos, les interactions avec les médias sociaux) jouait un rôle central dans les procédures du tribunal de la famille, particulièrement en ce qui concerne la communication concernant la garde, le droit de visite et l'échange (Koshan et coll., 2020). Dans le contexte de la pandémie de COVID-19, la technologie est devenue de plus en plus importante et sert de mécanisme principal pour faciliter les conversations se rapportant à la modification des ententes d'accès et d'échange et au bien-être de l'enfant ou des enfants pendant la pandémie.

Malgré les nombreux risques associés à la VCFT pour les survivantes et leurs enfants, il y a un manque de compréhension de la nature et du contexte de la question. Par conséquent, les idées fausses entourant la question présentent des défis importants pour les survivantes qui naviguent dans le système des tribunaux de la famille dans les cas de VCFT.

Ressources

Cette section présente plusieurs ressources en ligne se rapportant à la violence facilitée par la technologie, à l'hygiène numérique et à la planification de la sécurité. À moins d'indication contraire, les ressources sont en anglais.

BC Society of Transition Houses

Site Web : <https://bcsth.ca/techsafetytoolkit/>

La BC Society of Transition Houses a élaboré une *trousse d'outils en ligne sur la sécurité technologique et la protection des renseignements personnels* qui enseigne aux gens comment accroître la sécurité

Une étude réalisée en 2022 a révélé que les mères et les enfants sont souvent covictimes de la VCFT, malgré le fait que la communication facilitée par la technologie est perçue par le tribunal de la famille comme une solution de rechange plus sécuritaire que la communication en personne dans les relations impliquant la VC (Dragiewicz et coll., 2022). Les exigences imposées par les tribunaux concernant la communication au sujet de l'enfant (p. ex., donner des mises à jour par courriel, réaliser des ententes d'accès ou d'échange par message texte) peuvent présenter des situations dangereuses pour les mères en les mettant en contact direct avec leur agresseur. Les enfants peuvent transporter des appareils numériques entre chaque domicile parental, ce qui donne l'occasion à l'auteur de violence d'installer divers types de logiciels et de suivre l'emplacement de sa victime (Dragiewicz et coll., 2022). La VCFT peut aussi avoir une incidence négative sur le rôle parental dans les cas où les parents limitent les interactions en ligne de leurs enfants par crainte de la VCFT.

technologique et la protection de la vie privée. La trousse comprend une section sur la sécurité technologique générale, des conseils sur la sécurité des appareils et du matériel technologique, des conseils sur la sécurité lors de l'utilisation d'appareils intelligents, des conseils sur la sécurité et la protection des renseignements personnels en ligne, et d'éventuels recours juridiques en cas de violence facilitée par la technologie.

HackBlossom

Site Web : <https://hackblossom.org/domestic-violence/>

HackBlossom est une initiative qui vise à aider les survivantes de la VC à comprendre les menaces technologiques et les stratégies de protection.

Clinic to End Tech Abuse

Site Web : <https://www.ceta.tech.cornell.edu/resources>

Il s'agit d'un guide en ligne qui fournit des renseignements sur la façon de se déconnecter de partenaires ou d'ex-partenaires violents, de vérifier si les appareils contiennent des logiciels espions et d'autres applications cachées, et de sécuriser les comptes en ligne (p. ex., Gmail, Hotmail, Facebook et autres médias sociaux).

Projet déclic de YWCA

Site Web : <http://projectshift.ca>; Rapport sur le projet : <https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift-FR-Final-V4-Pages-BM.pdf>

Le site Web du Projet déclic fournit plusieurs guides qui se rapportent à la sécurité liée aux technologies. Par exemple, il y a un guide contenant des conseils et des outils pour aider les jeunes femmes et les filles victimes de cyberviolence; et un guide sur l'abus sexuel fondé sur l'image qui explique la nature du problème, les considérations juridiques, ainsi que les ressources et soutiens disponibles.

Feminist Frequency

Site Web : <https://onlinesafety.feministfrequency.com/en/#preventing-doxing>

Feminist Frequency est un guide en ligne sur le harcèlement en ligne et la divulgation de données personnelles (doxing).

CrashOverride

Site Web : <http://www.crashoverridenetwork.com>

CrashOverride est un projet créé pour promouvoir la sécurité en ligne et prévenir la violence en ligne. Le site Web comprend un centre de ressources offrant plusieurs guides utiles pour comprendre la violence facilitée par la technologie.

Trousse d'action de Toxic Hush

<https://www.informedopinionstoxichushkit.org/>

La trousse d'action de Toxic Hush vise à fournir du soutien et des ressources aux survivantes de la violence facilitée par la technologie et de la violence en ligne. Le site Web comprend également des renseignements à l'intention des allié.e.s et des personnes qui soutiennent les survivantes de la violence facilitée par la technologie.

Ressources – Sécurité des médias sociaux et retrait de la présence en ligne

HeartMob

Site Web : https://iheartmob.org/resources/safety_guides

HeartMob a élaboré un guide sur la sécurité des médias sociaux pour diverses plateformes, y compris Facebook, Instagram, Twitter, Reddit, Tumblr, Tiktok, Zoom et YouTube.

Cyber Civil Rights Initiative

Site Web : www.cybercivilrights.org/online-removal/

Le site Web de la Cyber Civil Rights Initiative comprend un guide pour retirer les images intimes des plateformes de médias sociaux.

Intel Techniques

Site Web : <https://inteltechniques.com/data/workbook.pdf>

Le site Web Intel Techniques comprend un carnet de travail qui énumère les étapes à suivre pour supprimer ses données personnelles qui sont disponibles en ligne.

Ressources – Identification et suppression des logiciels espions

Coalition Against Stalkerware

Site Web : <https://stopstalkerware.org/>

La Coalition Against Stalkerware est préoccupée par l'utilisation répandue de logiciels traqueurs et vise à lutter contre leur utilisation. Son site Web contient de courts guides à l'intention des entreprises de technologie, des médias et des survivantes.

Projets de recherche canadiens sur la violence facilitée par la technologie

CitizenLab

Le CitizenLab est un laboratoire interdisciplinaire basé à la Munk School of Global Affairs & Public Policy de l'Université de Toronto. Ses recherches portent sur l'espionnage numérique, les technologies émergentes et les répercussions sur la liberté d'expression, la vie privée, la sécurité et la surveillance.

Ses recherches sur la violence facilitée par la technologie ont produit deux rapports pertinents sur les logiciels traqueurs, disponibles ici : <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/>

The eQualityProject

The eQuality Project est basé à l'Université d'Ottawa. Ses recherches visent à mieux comprendre les expériences des jeunes en matière de protection de la vie privée et d'égalité dans un environnement de réseautage numérique, en mettant l'accent non seulement sur les actes individuels de VFT, mais aussi sur la façon dont les pratiques des entreprises exposent les jeunes aux conflits et au harcèlement.

Les documents de politique sont disponibles ici : <https://www.equalityproject.ca/policy/policy-papers/>
Les publications de recherche sont disponibles ici : <https://www.equalityproject.ca/research/research-publications/>

Fonds d'action et d'éducation juridique pour les femmes (FAEJ)

Les travaux du FAEJ sur la violence facilitée par la technologie rassemblent des avocats et des universitaires féministes pour étudier la question et imaginer des réponses juridiques possibles à la VFSFT. Plus récemment, le FAEJ a publié un rapport intitulé *Deplatforming Misogyny*, rédigé par Cynthia Khoo, qui examine les solutions juridiques possibles à la VFSFT sur les plateformes numériques.

Les documents du projet sont accessibles ici : <https://www.leaf.ca/project/tfv/>

Références

- Bailey, J. et Dunn, S. (24 novembre 2021). *La violence facilitée par la technologie : une introduction* [webinaire offert en anglais]. RESOLVE. Extrait de : <https://www.youtube.com/watch?v=GXL0qNfIWJ>
- BC Society of Transition Houses. (2014). *Technology misuse & violence against women: Survey* [infographie]. Extrait de : https://bcsth.ca/wp-content/uploads/2015/12/SNC_Tech_Misuse-Infograph2013-English.pdf
- BC Association of Transition Houses. (2022). *The technology safety and privacy toolkit*. Extrait de : <https://bcsth.ca/techsafetytoolkit/>
- Borrajo, E., Gámez-Gaudix, M., Pereda, N. et Calvete, E. (2015). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior*, 48, 358–65.
- Burlock, A. et Hudon, T. (2018). *Les femmes et les hommes ayant subi du cyberharcèlement au Canada*. Statistique Canada. Extrait de : <https://www150.statcan.gc.ca/n1/pub/75-006-x/2018001/article/54973-fra.htm>
- Dragiewicz, M., Woodlock, D., Salter, M. et Harris, B. (2022). “What’s mum’s password?”: Australian mother’s perceptions of children’s involvement in technology-facilitated coercive Control. *Journal of Family Violence*, 37, 137-149. <https://doi.org/10.1007/s10896-021-00283-4>
- Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview* (Supporting a Safer Internet, document n° 1). Centre pour l’innovation dans la gouvernance internationale (CIGI). Extrait de : <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/>
- Emezue, Chuka. (2020). Digital or digitally delivered responses to domestic and intimate partner violence during COVID-19. *JMIR Public Health and Surveillance*, 6 (3), 1-9. <https://doi.org/10.2196/19831>
- eQuality Project (2020). Technologically-facilitated violence: Criminal harassment case law. Extrait de : <http://www.equalityproject.ca/wp-content/uploads/2020/07/TFVAW-Criminal-Harassment-3-July-2020.pdf>
- Freed, D., Palmer, J., Minchala, D.E., Levy, K., Ristenpart, T. et Dell, N. (2017). Digital technology and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1 (46), 1-22.
- Gouvernement du Canada. (2021). *Qu’est-ce que la violence fondée sur le sexe?* Extrait de : <https://femmes-egalite-genres.canada.ca/fr/centre-savoir-violence-fondee-sexe/a-propos-violence-fondee-sexe.html>
- HackBlossom. (2022). *Defense strategies*. Extrait de : <https://hackblossom.org/domestic-violence/#defense>

- Hango, D. (2016). *La cyberintimidation et le cyberharcèlement chez les utilisateurs d'Internet âgés de 15 à 29 ans au Canada*. Statistique Canada. Extrait de : <https://www150.statcan.gc.ca/n1/pub/75-006-x/2016001/article/14693-fra.htm>
- Hinson, L., Mueller, J., O'Brien-Milne, L. et Wandera, N. (2018). *Technology-facilitated gender-based violence: What is it, and how do we measure it?* Washington, DC: International Center for Research on Women
- Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence*. Toronto (Ontario) : Fonds d'action et d'éducation juridique pour les femmes (FAEJ).
- Koshan, J., Mosher, J., Wiegers, W. (July 13, 2020). COVID-19, domestic violence, and technology-facilitated abuse. *ABlawg*. Extrait de : http://ablawg.ca/wp-content/uploads/2020/07/Blog_JK_JM_WW_COVID19_Surveillance.pdf
- Laxton, C. (2014). *Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking*. Bristol, Royaume-Uni : Women's Aid Federation of England. Extrait de : www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf.
- Ministère de la Justice. (2022). *Divorce et violence familiale* [fiche d'information]. Extrait de : <https://www.justice.gc.ca/fra/df-fl/fidvf-fsdfv.html>
- Šimonović, D. (2018). *Rapport de la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences concernant la violence en ligne à l'égard des femmes et des filles du point de vue des droits de l'homme*. Nations Unies. Extrait de : <https://digitallibrary.un.org/record/1641160?ln=fr>
- Slupska, J. et Tanczer, L.M. (2021). Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things (p. 663-688). Dans [Bailey, J.](#), [Flynn, A.](#) and [Henry, N.](#) (Dir.) *The emerald international handbook of technology-facilitated Violence and Abuse*. Emerald Publishing Limited: Bingley, Royaume-Uni. Extrait de : <https://doi.org/10.1108/978-1-83982-848-520211049>