NOUVELLES TECHNOLOGIES ET VIOLENCE CONJUGALE

Outils facilitateurs de violence et de renforcement du contrôle coercitif

CRPC | Chaire de recherche en prévention de la cybercriminalité

Auteure

Isabelle Chadic, candidate à la maîtrise en criminologie

Révision

Fyscillia Ream, coordonnatrice scientifique de la Chaire de recherche en prévention de la cybercriminalité

Benoît Dupont, titulaire de la Chaire de recherche en prévention de la cybercriminalité

Pour citer: Chadic, I.(2023). *Nouvelles technologies et violence conjugale. Outils facilitateurs de violence et de renforcement du contrôle*. Rapport de recherche. Chaire de recherche en prévention de la cybercriminalité.

Ce document est disponible intégralement en format électronique (PDF) sur le site Web de la Chaire de recherche en prévention de la cybercriminalité à : https://www.prevention-cybercrime.ca.

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Sommaire exécutif

Le développement des nouvelles technologies au cours des trois dernières décennies a grandement modifié notre manière de concevoir les relations interpersonnelles. En quelques clics, nous pouvons désormais faire de nouvelles rencontres, suivre en temps réel les activités réalisées par nos proches ou bien encore partager nos bons moments. Or, l'augmentation des crimes liés aux nouvelles technologies démontre le potentiel préjudiciable des technologies de l'information et des communications (TIC) particulièrement dans les cas de violences conjugales où elles alimentent les opportunités de violences et de contrôle envers les victimes[1, 2].

Plusieurs organismes communautaires, et chercheurs universitaires reconnaissent que l'utilisation des nouvelles technologies dans les cas de violences conjugales ne cesse d'augmenter[1, 2, 3]. Des chercheurs ont démontré que certaines caractéristiques des violences conjugales telles que « la durée, l'intensité et le caractère envahissant » ont un effet décuplé lorsque des outils technologiques sont utilisés à des fins malveillantes[4].

Ce rapport de recherche met en lumière les différentes formes de violence facilitées par les technologies, allant du cyberharcèlement aux cyberviolences à nature sexuelle. De plus, les différents outils et technologies utilisées en violence conjugale y sont également présentés. La diversité, le caractère invasif ainsi que les capacités de ces différentes technologies permettent d'illustrer l'étendue des outils disponibles aux partenaires violents.

Dans un contexte de violence conjugale facilitée par les technologies, la sécurité des victimes ne doit pas passer par une suppression ou une limitation de l'utilisation des technologies par les victimes, mais plutôt viser l'autonomisation de ces dernières. Dans ce contexte, les conseils de cybersécurité actuels sont moins propices aux victimes et peuvent même conduire à des effets inverses. Des efforts spécifiques doivent être mis en œuvre pour aider les victimes à lutter contre le cycle de cyberviolence et reprendre le contrôle de la situation. Nous proposons quelques pistes de réflexion de stratégie possible dans la lutte contre les cyberviolences: la création de campagnes de sensibilisation à plusieurs niveaux, l'offre de formation continue sur l'utilisation des technologies en violence conjugale, la mise en place d'un groupe de travail spécialisé sur l'utilisation des technologies dans les violences faites aux femmes et la création de dispositifs identifiant les intrusions technologiques malveillantes.

Table des matières

Introduction

Le développement des nouvelles technologies au cours des trois dernières décennies a grandement modifié notre manière de concevoir les relations interpersonnelles. En quelques clics, nous pouvons désormais faire de nouvelles rencontres, suivre en temps réel les activités réalisées par nos proches ou bien encore partager nos bons moments. Or, l'augmentation des crimes liés aux nouvelles technologies démontre le potentiel préjudiciable des technologies de l'information et des communications (TIC).

Ce potentiel est particulièrement observé dans les cas de violences conjugales où les technologies alimentent les opportunités de violences et de contrôle envers les victimes [1, 2]. Ces violences facilitées par les technologies se regroupent sous le terme «**cyberviolences**» et se définissent comme «**l'utilisation des technologies pour harceler, surveiller, contrôler ou exercer des pressions sur un partenaire ou un ancien partenaire**» [3]. Des chercheuses ont relevé que près de 78 % des victimes de violences conjugales ont vécu des événements de cyberviolences [4]. Une autre étude rapporte quant à elle, une augmentation de 420 % des signalements de violences conjugales facilitées par les technologies durant la pandémie de la COVID-19 [5].

Dans les cas de cyberviolences, les TIC sont à la fois utilisées par les partenaires violents afin de renforcer les mécanismes de contrôle, mais également par les victimes, comme moyen de dénonciation et comme outils de protection contre les abus [6].

Il importe d'avoir une meilleure compréhension de l'utilisation malveillante des TIC par les partenaires violents afin de mieux outiller les victimes et les intervenants. En effet, l'omniprésence de ces technologies dans la vie quotidienne des individus rend difficile pour les victimes le maintien d'une utilisation sans risque à l'abri de l'emprise du ou de la partenaire violent.e [7].

En outre, il est nécessaire de se pencher sur une stratégie d'autonomisation, s'appuyant sur la prévention, la dénonciation ou même la réparation, où les victimes et leurs aidants pourront utiliser à leur tour la technologie afin de lutter contre le cycle de cyberviolence et reprendre le contrôle de la situation [6]. Cette étude a été réalisée afin de brosser un portrait des cyberviolences perpétrées dans un contexte de relations intimes. Dans un premier temps, nous mettrons en avant la problématique avant d'aborder les types de violences facilitées par les technologies et les différents outils qui sont utilisés. Finalement, nous présenterons des recommandations afin d'améliorer la réponse à ce problème.

Les violences conjugales sous un autre jour

Une évolution constante

Plusieurs organismes communautaires et chercheurs universitaires reconnaissent que l'utilisation des nouvelles technologies dans les cas de violences conjugales ne cesse d'augmenter, d'où la nécessité de se pencher sur la question [8, 9, 10]. Des chercheurs ont démontré que certaines caractéristiques des violences conjugales telles que « **la durée, l'intensité et le caractère envahissant** » ont un effet décuplé lorsque des outils technologiques sont utilisés à des fins malveillantes [11]. En cela, **les nouvelles technologies ont non seulement changé la façon dont les violences conjugales sont perpétrées, mais également créées de nouvelles opportunités** [11]. De nos jours, un simple téléphone intelligent suffit à un partenaire pour exercer un contrôle coercitif envers son ou sa conjoint. e [8]. Malheureusement, alors que plus en plus d'outils technologiques sont développés ou utilisés à des fins malveillantes dans les cas de violence conjugale, il devient extrêmement difficile pour les victimes d'y échapper.

L'évolution rapide des technologies rend difficile l'adoption de réflexes cybersécuritaires pour les victimes de cyberviolences et les intervenants du milieu. En effet, les partenaires intimes disposent d'une panoplie d'outils et d'applications numériques pour exercer un contrôle coercitif sur les victimes. Une équipe de recherche de l'University College London souligne que les partenaires violents ont tendance à avoir une longueur d'avance sur leurs victimes, car ils ont connaissance des possibilités offertes par les outils technologiques pour exercer un contrôle sur leur victime couplée à une intention malveillante [12]. De ce fait, de nombreuses victimes sont enclines à partager leurs localisations, mots de passe, NIP de carte bancaire et autres informations liées aux technologies avec leur partenaire violent afin d'éviter les représailles en cas de refus [13].

Des intervenants dépassés

Les intervenants en violence conjugale se retrouvent inévitablement dépassés par la complexité des outils technologiques utilisés à l'encontre des victimes. Mis à part quelques connaissances telles que la désactivation de la localisation ou le retrait de la carte SIM sur l'appareil de la victime, **les intervenants en maisons d'hébergement ne**

possèdent pas de procédures uniformisées pour gérer les aspects technologiques lors de l'accueil des victimes, problème amplifié par un grand roulement de personnel [14]. Parallèlement, les intervenantes soulignent que les victimes ont tendance à banaliser la sécurité de leurs informations et de leurs appareils, diminuant ainsi leur résilience face à la cybersécurité [14]. Par exemple, les victimes estiment peu important de changer leurs mots de passe ou de désactiver leur localisation lorsqu'elles arrivent en maison d'hébergement, car elles ne considèrent pas de danger imminent [14]. **Pour les intervenants, se pose également l'enjeu de la sécurité de l'organisme accueillant la victime de violence conjugale** puisque si cette dernière est suivie et surveillée par son ex-partenaire, cela crée un réel danger pour les autres occupants de la maison d'hébergement [15]. Le recours aux TIC dans les cas de violence conjugale fait donc partie d'une réalité à laquelle les intervenants des maisons d'hébergement sont de plus en plus confrontés et à laquelle ils et elles ne sont pas préparés.

Le cyber et la justice

Les partenaires intimes n'ont pas besoin de grandes connaissances en informatique pour utiliser les nouvelles technologies afin d'exercer un contrôle envers leur partenaire tout en préservant leur anonymat aussi bien lors d'une relation en cours que dans un contexte post-séparation [2]. L'anonymat perçu que procurent les nouvelles technologies leur permet notamment de se déresponsabiliser et d'échapper ainsi aux sanctions reliées à leurs gestes préjudiciables [6]. Il devient donc difficile pour une victime d'obtenir réparation pour des crimes commis par l'entremise de technologies, et ce, notamment dans le cas des cyberviolences, qui ne sont pas aussi facilement prises en charge par les forces de police et dont les réponses policières peuvent varier [16]. Ce constat est valable pour la cybercriminalité de manière générale où la réponse policière reste encore faible pour certains types de crime comme les fraudes en ligne. Dans le cas des cyberviolences, les difficultés à constituer une preuve du délit empêchent les policiers d'agir [15]. On peut donc observer un fossé entre les forces de l'ordre et les maisons d'hébergement dans la réponse aux cyberviolences et la prise en charge des victimes. En outre, une autre difficulté à laquelle doivent faire face les victimes de cyberviolences est la publication d'informations personnelles et/ou de photos intimes à leur insu sur le web, ce qui implique un aspect de permanence et de propagation rapide dont la résolution, à savoir faire supprimer ce contenu en ligne, est presque inexistante [14]. Par exemple, les sites de *revenge porn* refusent fréquemment les demandes des victimes quant aux retraits des photos et d'informations les concernant [16]. Ces aspects nuisent non seulement au sentiment de justice, mais également au rétablissement d'une victime de violence conjugale [4].

Cyberviolences: directes et indirectes

Fernet et ses collègues ont conceptualisé la cyberviolence selon deux aspects, soit leur caractère **direct** ou **indirect**, caractère qui dépend de la motivation du partenaire violent et des moyens technologiques utilisés. **Les cyberviolences directes** présentent un caractère privé et direct en regard du partenaire/ex-partenaire victimisé [4]. Les actes perpétrés par le conjoint violent et facilités par la technologie relèvent de la sphère privée de la victime et ne deviennent publics que s'ils sont dévoilés par cette dernière [4]. Par exemple, les messages textes harcelants d'un partenaire violent constituent des actes de cyberviolences directes. **Les cyberviolences indirectes** se produisent lorsque le partenaire/ex-partenaire décide d'exposer au grand public du contenu ou des informations au sujet de la victime, dans le but de lui porter préjudice. Ce contenu peut être à caractère sexuel ou simplement porter atteinte à la réputation de celle-ci ou encore les deux, comme cela est en est le cas dans le *revenge porn* [4].

Les différentes formes de violences facilitées par les technologies

Cyberharcèlement

Le **cyberharcèlement** se définit comme «**l'utilisation répétée d'un moyen de communication électronique afin de harceler ou d'effrayer une autre personne**» [17]. De plus, le cyberharcèlement est entrepris afin d'instaurer de la peur chez la victime et que, dans un contexte de violence conjugale, le risque d'exécution des menaces perpétrées en ligne se trouve être plus élevé [11].

Par exemple, le partenaire violent peut envoyer à sa victime une multitude de messages et/ou d'appels inquiétants, dégradants et menaçants en l'espace de quelques secondes et ce, sur une courte période et de façon continue. Le partenaire peut également publier de fausses informations sur les réseaux sociaux à propos de la victime, se créer de faux profils sur des sites pornographiques afin de se faire passer pour la victime ou bien encore publier des informations personnelles [18].

Ça pourrit la vie de la femme harcelée et surveillée en créant une véritable psychose, car lorsqu'elle s'en rend compte, elle commence à douter de tout et à n'avoir plus confiance en rien [19]

Surveillance et contrôle facilités par les technologies

La **cybersurveillance** et le **contrôle facilité par les technologies** se définissent comme «**l'utilisation des technologies ou des données hébergées en ligne pour obtenir de l'information au sujet d'un partenaire actuel ou d'un ancien partenaire intime, afin de savoir notamment ce qu'il fait, où il se trouve et avec qui**» [3]. Ces informations permettent généralement d'exercer de l'influence et du contrôle sur le partenaire ou l'ex-partenaire [2]. Cette forme de violence peut inclure la surveillance sur les réseaux sociaux, le recours à des dispositifs GPS, la visualisation de l'historique d'un compte bancaire afin de localiser sa victime ainsi que le recensement des habitudes d'achat. La surveillance en ligne peut être également utilisée à des fins sexuelles dans les cas de voyeurisme ou bien encore de prise de photos explicites à l'insu de la victime [2].

La surveillance peut également escalader et prendre place dans le monde physique en y incluant du harcèlement, la profération de menaces, ou encore de la violence physique [20].

À travers l'utilisation de divers moyens technologiques, le partenaire violent exerce son contrôle par **la restriction des diverses activités quotidiennes de sa victime** [2]. Par exemple, lorsque le partenaire contrôle l'accès au compte bancaire de sa victime, cette dernière ne peut accéder à ses fonds pour se déplacer, faire ses courses ou toute autre activité qui lui sont nécessaires [21]. Cette forme de contrôle est extrêmement préjudiciable, dans la mesure où elle entraîne des conséquences, telles que l'isolement, et peut donc priver la victime de son système de soutien [22]. De nombreuses séquelles psychologiques peuvent également survenir telles que l'anxiété, la dépression, la paranoïa, la honte ou bien encore la peur [22].

« Partout où j'allais, il était là [...] Il sortait devant moi. Je sors des magasins, il était là ». Finalement, elle a découvert pourquoi : des AirTag d'Apple étaient cachés à deux endroits, y compris sa voiture [23]

Cyberviolence sexuelle

Les **cyberviolences sexuelles** impliquent les « **comportements visant à forcer un (ex) partenaire à acheminer ou faire la réception de contenu à caractère sexuel par l'entremise des technologies ou à faire pression pour que le partenaire s'y plie** » [3]. Les cyberviolences sexuelles peuvent être commises par l'entremise des technologies de l'information telles que les réseaux sociaux ou encore par textos ou appel visio [24].

Revenge porn

Les dernières données de Statistique Canada rapportent une augmentation des cas de *revenge porn* : le nombre d'affaires de distribution non consensuelle d'images intimes a augmenté de près de 9 % en 2021 par rapport à l'année précédente, ce qui représente une hausse de 52 % en comparaison avec la moyenne des cinq années précédentes [25]. Le *revenge porn* implique « **le partage non consensuel d'images intimes avec ou sans positions sexuelles explicites, sur lesquelles peuvent être représentées des partenaires ou d'ex-partenaires** » [26]. Ce type d'actes a pour but d'humilier la victime, par la publication de photos et vidéos intimes identifiant cette dernière, et ce, afin qu'elle puisse faire l'objet de harcèlement subséquent de la part d'inconnus [16]. La distribution non consensuelle d'images intimes peut se faire de plusieurs façons : elles peuvent être

envoyées directement à des amis, des membres de la famille, des employeurs ou être publiées en ligne [16]. Généralement, le *revenge porn* se produit dans un contexte de post-séparation difficile [26]. Toutefois, le partage non consensuel d'images intimes peut également survenir dans le cadre d'une relation en cours [27]. Ainsi, le terme « **abus sexuel fondé sur l'image** » (« image-based sexual abuse » en anglais), serait plus approprié pour identifier cette pratique, car il met non seulement l'emphase sur l'aspect abusif de cette pratique, mais également les impacts sur les victimes et non pas seulement les motivations des délinquants [27].

Les gens savent où je travaille, où j'habite, la ville d'où ça vient, mon nom au complet et mon visage sont dans les photos. Vraiment, je ne me sens pas en sécurité ! [29]

Sextorsion

La **sextorsion** implique « **la menace de diffusion d'images explicites, intimes ou embarrassantes à caractère sexuel sans consentement, généralement dans le but de se procurer des images supplémentaires, des actes sexuels, de l'argent ou autre chose** » [28]. Selon la conceptualisation des cyberviolences Fernet et ses collègues, la sextorsion peut être considérée comme une violence directe, car les menaces sont proférées directement à la victime et dans un contexte privé ce qui offre aux abuseurs l'opportunité d'exercer une emprise sur leur victime [4]. En outre, le caractère privé des menaces permet de différencier la sextorsion du *revenge porn*, lorsque les menaces de diffusion ne sont pas mises à exécution [28].

Technologies utilisées à des fins de violence conjugale

La création de faux comptes sur les réseaux sociaux

Utilisée aux différents stades de la relation, **la création de faux comptes est un moyen fréquemment employé par les partenaires abusifs** [2]. Il suffit généralement d'un courriel et de quelques informations inventées de toute pièce afin de remplir le formulaire d'inscription sur la plateforme de réseau social [2]. Le partenaire peut créer une nouvelle identité, en usurper une ou bien encore usurper celle de la victime [2]. Le manque de vérification de l'identité des utilisateurs par les plateformes de réseaux sociaux bénéficie aux partenaires violents qui recourent à ces moyens d'autant plus qu'ils permettent de maintenir les violences conjugales, et ce, même lorsque la relation est terminée [16, 26]. Les prochaines sections feront état des différentes motivations sous-tendant l'utilisation des faux comptes par le partenaire.

La surveillance

Le faux compte peut être créé afin de suivre les faits et gestes de la victime, sans entrer en contact avec celle-ci [2]. Dans ces cas, le partenaire utilisera l'identité d'une personne généralement inconnue de la victime afin que la demande d'ami ou d'abonnement soit acceptée et de passer inaperçu. Une fois la demande acceptée, le partenaire utilisera l'identité d'une personne généralement inconnue de la victime afin que la demande d'ami ou d'abonnement soit acceptée et de passer inaperçu. Une fois la demande de connexion acceptée, le partenaire adoptera un comportement passif lui permettant d'observer la vie de sa victime [26]. Cette surveillance permet non seulement d'exercer une certaine forme de contrôle tout en conservant l'anonymat. Grâce aux informations collectées, le partenaire peut non seulement être en mesure de localiser quotidiennement son ex-conjoint.e, mais également les utiliser à des fins de menaces, d'intimidation ou tout autre type de violence pouvant nuire à la sécurité de la victime.

Conserver un moyen de contact

Un faux compte peut être créé par l'ex-partenaire afin d'entrer en communication avec la victime. Dans ce cas, le partenaire utilise généralement l'identité d'un inconnu ou d'une connaissance de la victime[2]. À l'aide du faux compte, l'ex-conjoint peut tenter

d'entamer une relation avec l'ex-partenaire afin de regagner son amour. Dans les cas où les partenaires sont toujours en relation, le faux compte peut être utilisé afin de tester le ou la partenaire et le potentiel d'adultère [2]. Si le ou la partenaire répond aux sollicitations du faux compte, le partenaire violent peut utiliser cette information afin de blâmer la victime pour sa participation à la discussion [2] et justifier de possibles autres mesures de surveillance et de coercition. La prise de contact peut également viser à acheminer des messages haineux [16]. Lorsque les messages sont abusifs, la victime peut bloquer le compte et ainsi, engager le partenaire à générer plusieurs faux comptes à la fois afin de perpétuer le harcèlement [16].

L'atteinte à la réputation

Certains partenaires violents utilisent les TIC pour **porter préjudice à l'intégrité de leur victime en ternissant l'image de ces dernières sur les réseaux sociaux** [2]. Pour ce faire, ils peuvent recourir à l'identité d'un inconnu, d'un compte anonyme ou encore usurper l'identité de leur victime [2]. Les partenaires utilisent alors ces comptes pour publier des images intimes de la victime à son entourage, publier des messages dégradants sur la victime, et nuire aux relations interpersonnelles avec ses proches [16]. Les partenaires usurpent l'identité de leur victime lorsqu'ils ne possèdent pas les compétences informatiques pour pirater le compte de la victime [2]. La majorité des faux comptes usurpant l'identité des victimes est utilisée sur les sites de rencontre afin d'alimenter des conversations sexuelles avec d'autres utilisateurs tout en communiquant de véritables informations personnelles (adresse, numéro de téléphone, etc.). La victime recevra donc par la suite, des appels, message texte ou bien encore des visites de personnes pensant avoir discuté avec elle sur les sites de rencontre [2].

On travaille avec une fille de 14 ans dont le copain a créé de faux comptes Facebook et a posté des photos d'elle nu après avoir invité tous ses amis et famille à être "amis"[30]

L'accès aux comptes: via le droit de propriété ou de non-autorisée

Accès via le droit de propriété

L'accès aux appareils et aux comptes des victimes peut se faire sous prétexte que **le partenaire violent détient le statut légal de propriétaire d'un appareil** (lorsqu'il procède à l'achat de l'appareil) **ou d'un compte** (bancaire, par exemple) [8, 13]. Ce type d'accès est

utilisé pour empêcher la victime de physiquement utiliser un appareil ou un compte si cette dernière souhaite demander de l'aide [13]. Par exemple, si la victime tente d'appeler la police, le partenaire violent peut lui contraindre de lui remettre l'appareil en se déclarant être le propriétaire du téléphone. Ce droit de propriété s'exprime également sous forme de contrôle numérique, par exemple, en changeant le mot de passe du routeur et en coupant l'accès à Internet sur le téléphone de la victime lorsque le partenaire violent est le propriétaire de la ligne téléphonique du domicile [13]. Ce type de contrôle permet aux conjoints violents de suivre et surveiller la victime et contrôler l'usage de ses appareils et accès Internet via les plans familiaux du fournisseur Internet [13]. Par exemple, les factures de téléphonie peuvent fournir plusieurs renseignements détaillés sur l'historique des communications effectuées par la victime [13].

Les appareils électroniques des enfants peuvent également être utilisés à des fins de surveillance et contrôle notamment lors d'une séparation, lorsque la victime a quitté le lieu de vie commune avec les enfants [13]. Un partenaire violent peut légalement, être en droit de contacter ses enfants et au-delà de ce contact, pouvoir avoir accès à la victime. De plus, les partenaires violents profitent de leur droit de propriété afin d'accéder à différents services de sauvegarde de données offerts par les compagnies de téléphonie ou de services Internet [13]. Ces services offrent, entre autres, la configuration de transmission automatique de toutes les données liées à un appareil vers le « nuage » comprenant les messages textes, photos ou bien encore données de localisation, ce qui permet de surveiller continuellement la victime [13]. Les ex-conjoints peuvent ainsi utiliser les services de localisation de l'infonuagie comme « Find my friend » ou « Find my iPhone » pour les utilisateurs d'Apple [13].

> *[L'ex-partenaire] avait acheté le téléphone chez [fournisseur de téléphonie], c'était son compte . . . Il peut voir toutes les personnes à qui je parle. Il a certainement accès à ma boîte vocale. Je viens juste d'apprendre que quelqu'un d'autre peut accéder à ma boîte vocale[13]*

Accès non autorisés aux comptes

L'accès non autorisé aux comptes représente également un moyen utilisé pour maintenir une emprise sur la victime[13]. Le partenaire peut accéder aux comptes en forçant la victime à divulguer ses mots de passe ou en les devinant[2, 13]. Il n'est pas rare que dans le cours d'une relation, deux conjoints partagent les mots de passe de différents comptes

(bancaires, réseaux sociaux, courriel, etc.) lorsqu'il existe un lien fort de confiance. Ces informations peuvent être partagées entre les conjoints, enregistrées dans un gestionnaire de mot de passe commun, devinées (si on connaît bien la personne), ou obtenues par coercition [2, 13]. En effet, la victime peut être forcée de donner ses identifiants sous la menace de violence physique ou même psychologique [8]. Dans d'autres cas, les partenaires violents vivant avec leur victime ont accès aux appareils déverrouillés cette dernière et peuvent donc en profiter pour prendre note des identifiants des différents comptes qu'elle possède [13].

L'accès non autorisé aux comptes comporte des buts précis tel que de modifier les informations personnelles permettant de bloquer un futur accès aux victimes, modifier la configuration de l'authentification à double facteur et rendre impossible la récupération du compte pour la victime, supprimer des contacts, surveiller les communications des victimes ou bien encore sauvegarder les coordonnées de la liste de contact de sa victime afin de l'utiliser pour la rejoindre en cas de coupure de contact [8, 13].

Les dispositifs de localisation

Existant sous plusieurs formes, les **« trackers » commerciaux** permettent normalement de retrouver des objets perdus (clés, portefeuille, sac, etc.). Or, différents services de police et organismes ont rapporté le recours grandissant à ces dispositifs dans les cas de violence conjugale ou de harcèlement [30]. En effet, **ces appareils facilitent le suivi des déplacements d'une personne en fournissant des données de géolocalisation extrêmement précises** [31].

D'ailleurs, un sondage dans 70 maisons d'hébergements pour victimes de violence conjugale aux États-Unis montre que 85 % d'entre elles ont eu à faire à des victimes qui ont été suivies par leurs partenaires violents via des systèmes GPS [32]. Certaines des victimes auraient même affirmé que les conjoints auraient sciemment offert des téléphones cellulaires de type iPhone comme cadeau de Noël à leurs enfants afin de pouvoir suivre la victime durant et après la séparation [32].

Les dispositifs de localisations se présentent sous deux formes, **passifs** ou **actifs** [31]. **Les « trackers » actifs** sont programmés afin de transmettre continuellement des données de localisation au propriétaire [31]. **Les « trackers » passifs** transmettent uniquement de l'information à la demande du détenteur du dispositif ou à intervalles réguliers lors de mouvements [31].

Le partenaire violent peut **placer le dispositif dans la voiture, dans le sac ou tout autre objet utilisé quotidiennement par la victime** et ainsi, suivre les déplacements de cette dernière depuis son téléphone [33]. Les dispositifs sont également **dissimulés dans des jouets pour enfants** car ces objets sont conçus de façon à être discrets, étant de petite taille et très légers les rendant difficilement repérables par la victime [31, 33]. Selon la marque de l'outil, les données sont disponibles en quelques heures ou quelques jours [31].

Chaque dispositif fonctionne différemment. Par exemple, le AirTag d'Apple utilise les signaux Bluetooth. Le AirTag ne possède pas de système GPS c'est-à-dire que la localisation ne s'appuie pas sur les données satellites. Au contraire, le fonctionnement repose sur les données de localisation des appareils Apple à proximité [34]. Le AirTag lance un signal Bluetooth sécurisé, capté par les appareils connectés aux réseaux à proximité. Chaque appareil soumet ensuite sa localisation à iCloud, permettant de situer l'objet sur la carte dans l'application « Find My » d'un appareil Apple, la mise à jour des données de localisation se fait plus rapidement que lorsqu'il se trouve dans un endroit désert. En effet, s'il n'y a pas d'appareils Apple à proximité, il sera impossible pour l'Air Tag de transmettre les données de localisation à iCloud, et donc, à son propriétaire [34].

Parallèlement, les GPS de type automobile peuvent également être utilisés à des fins de géolocalisation [31]. En effet, ces derniers conservent un historique des endroits visités auquel le partenaire peut facilement y avoir accès [31]. La majorité des traceurs GPS disposent d'une carte SIM et de micros intégrés permettant de fournir les données de localisation, et ce, en croisant les données satellites à celles du réseau mobile [31]. Certains GPS sont également munis de systèmes de géo-clôture, une fonctionnalité délimitant une zone prédéfinie de navigation et dont le dépassement génère des alertes au détenteur du compte [35]. Les déplacements de la victime se retrouvent donc totalement surveillés de manière automatisée.

Les objets intelligents connectés (IoT)

Les objets intelligents connectés sont des dispositifs physiques auxquels un système informatique et une connexion Internet ont été implantés afin d'offrir de meilleures fonctionnalités aux utilisateurs [36]. Ces objets font partie intégrante de l'**Internet des objets** (« Internet of Things [IoT] » en anglais). L'IoT est « **un réseau ouvert et complet d'objets intelligents qui ont la capacité de s'organiser automatiquement, de partager des informations, des données et des ressources, de réagir et d'agir face aux situations et aux changements de l'environnement** » [37]. Cette avancée technologique permet donc aux utilisateurs de contrôler leurs objets à distance (ex. démarrer une cafetière à l'aide de son appareil téléphone) [38]. Il existait plus de 50 milliards d'objets intelligents connectés en 2020 [39].

Il faut s'attendre à voir **plus de 125 milliards d'objets IoT pouvant être utilisés à mauvais escient dans un contexte de violence conjugale** [40]. Les objets connectés ont la capacité de surveiller visuellement, géographiquement et de manière auditive, les partenaires victimes [41, 42]. En outre, la popularité de ces appareils a mené les développeurs de produits à offrir la fonctionnalité de la multiplicité des comptes, ce qui permet à plusieurs individus d'accéder au même appareil. Dans un contexte de violence conjugale, le partenaire violent peut décider d'être administrateur de tous les appareils, ce qui lui permet d'exercer un contrôle total sur ces derniers [41, 43].

Les appareils IoT peuvent être utilisés par les partenaires violents de diverses manières [38]. En 2018, une enquête menée par entrevue sur la prévalence des violences facilitées par l'IoT ont permis de relever plusieurs stratagèmes : **airs climatisés éteints à distances, codes d'accès numériques des portes d'entrée constamment modifiés, activation des sonnettes en continu sans présence d'un individu, changement de température dans les maisons, mise en marche d'une bouilloire électrique et bien d'autres encor**e [44]. D'autres comportements ont été rapportés tels que : l'utilisation des capteurs intelligents sur les portes de la maison afin de vérifier les entrées et sorties de la victime, le contrôle des serrures intelligentes pour empêcher la victime de sortir de la maison, ou bien encore la surveillance des historiques de recherche des assistants virtuels contrôlés par la voix [43]. Ces diverses utilisations agissent sous forme de violence psychologique ayant pour but de semer le doute dans la perception de la réalité de la victime, érodant son estime de soi et augmentant leur dépendance envers le partenaire violent [45].

Les lumières de ma maison ne cessent de s'allumer et de s'éteindre sans que je fasse quoi que ce soit [43]

Caméras et microphones cachés dans les appareils pour enfants

Les partenaires violents peuvent également **implanter dans les jouets des enfants du couple des dispositifs technologiques** tels que des caméras ou des micros pour garder une trace, presque en temps réel, des activités de la victime. D'ailleurs, lesdits dispositifs sont facilement accessibles sur des sites de vente en ligne tels qu'eBay et Amazon [2]. Il est également possible de les implanter sur d'autres objets tels que les poussettes ou les sièges auto. Ce faisant, les enfants et leurs objets deviennent un moyen indirect d'atteindre la victime [33].

Les logiciels et applications

Les maliciels

Les principaux maliciels utilisés en contexte de violence conjugale sont de type **logiciel espion** («spyware» en anglais) et permettent aux partenaires violents d'accéder aux fonctionnalités de l'appareil de la victime telles que sa caméra et son microphone afin de la suivre, la surveiller et la contrôler [46, 47]. Les logiciels espions « **donnent accès à toutes les actions effectuées avec l'appareil : les appels, les messages, les courriels, les photos, les éléments supprimés, les sites Internet visités, les habitudes d'achat et permettent la géolocalisation de l'utilisateur de l'appareil** » [4, 48]. Initialement, ces logiciels étaient utilisés par des agences gouvernementales d'application de la loi pour leurs activités de surveillance et d'espionnage [49]. Commercialisés, ces logiciels sont devenus plus accessibles au grand public et peuvent être donc utilisés à des fins malveillantes par tout un chacun [50]. Il est possible de se procurer illégalement ces logiciels sur l'AppStore et Google Play [46]. Ils sont également téléchargeables sur des sites d'application alternatifs tels que Cydia, une application qui permet de télécharger des applications non autorisées par Apple et ne se retrouvant donc pas sur l'App Store officiel [32, 51].

Les logiciels espions peuvent être installés sur l'appareil sans qu'il n'y ait aucune icône visible témoignant de leur présence, ou avoir l'apparence d'une application non alarmante, voire légitime, rendant difficile la détection pour les victimes [52]. D'ailleurs, la majorité des logiciels anti-espion disponibles sur le marché détectent difficilement les logiciels espions sur les appareils et il est donc difficile pour les victimes de savoir véritablement si ces derniers sont infectés [46]. Les logiciels malveillants peuvent être installés à distance ou via un objet physique et seule la connaissance du mot de passe de l'appareil de la victime est suffisante pour son installation [52].

Plusieurs exemples de procédure utilisant des objets physiques telle que le Rubber Duckie ont été rapportés [47]. Possédant l'apparence d'une clé USB tout à fait normale, le dispositif vole en 15 secondes les mots de passe stockés sur un ordinateur, et ce même s'il est protégé par un mot de passe. Il est discret et ne nécessite aucune action particulière si ce n'est d'insérer l'objet dans un port USB [47]. Un autre dispositif physique malveillant est le « Tortue LAN » qui, lorsque connecté à un port USB est utilisé pour l'interception de l'ensemble trafic réseau. En d'autres mots, il permet à un partenaire violent d'accéder à distance à toute donnée passant sur ledit réseau et ainsi surveiller ou bien encore dérober des informations à sa victime [47].

L'installation à distance peut se faire à travers l'hameçonnage, en envoyant un courriel frauduleux contenant des pièces jointes infectées [14]. D'autres stratagèmes tels que de faux courriels de notifications de tentative de connexion ou des factures diverses sont également mis en place [47]. Ces courriels redirigent les victimes vers un lien qui les invitera à entrer des informations personnelles tels que leur mot de passe [47]. D'ailleurs, parfois, la simple ouverture du courriel est suffisante pour exécuter le logiciel. Il est également possible d'inclure le programme malveillant dans une pièce jointe infectée sous forme de fichier, image, ou vidéo. De cette façon, dès que la personne ciblée clique sur la pièce jointe, le programme s'exécute automatiquement [32]. Ces procédés peuvent être utilisés par les partenaires violents pour accéder aux appareils de la victime et y installer des maliciels ou logiciels espions ou bien encore pour des raisons d'abus psychologiques.

Logiciels légitimes utilisés à des fins malveillantes

La mystification de l'identité de l'appelant

La **mystification de l'identité de l'appelant** (aussi appelée « Caller ID spoofing » en anglais), représente «**le fait de modifier l'identité de l'appelant affichée pour la personne qui reçoit l'appel**» [53]. La mystification de l'identité de l'appelant peut être utilisée à des fins légitimes, par exemple dans le cas d'un médecin qui souhaiterait informer un patient des résultats d'une analyse par téléphone, en affichant le numéro générique de rappel d'un centre hospitalier en tant qu'appelant, et ce, afin de s'assurer que de futures demandes soient convenablement dirigées. Les individus malveillants utilisent l'identité d'institutions ou de personnes de confiance afin d'inciter une victime à répondre à l'appel [54]. En contexte de violence conjugale, les partenaires violents utilisent cette technique afin de rejoindre leur victime afin d'outrepasser leurs ordonnances d'interdiction de communication ou tout simplement pour s'assurer que la victime réponde aux appels en se faisant passer par exemple pour un membre de la famille ou d'un employé de la justice [55, 56].

Cette technique a également un effet dévastateur au niveau psychologique et émotionnel puisque le partenaire violent peut utiliser à répétition la mystification de l'appelant et créer de l'angoisse, de l'anxiété et de la peur chez la victime à chaque fois que son téléphone sonne [55].

Les services de mystification de l'appelant sont disponibles sur le web tels que spoofmyphone.com, spoofcard.co, spooftel.com, bluffmycall.com. Par exemple, spoof my phone requiert de fournir un faux numéro créé de toute pièce ainsi qu'un vrai numéro. Le site offre même l'option de changer la voix ainsi qu'ajouter des effets spéciaux.

Spoof my phone offre également des services de messages textes, courriel ou Whats App frauduleux par le biais d'applications partenaires telles que Spoof my text, Spoof my email et Spoof my WhatsApp. De plus, spoofing.com assure à ses clients que leurs appels et informations sont cryptés via le protocole sécurisé HTTPS (SSL, Secure Sockets Layer) afin de rendre l'accès aux informations impossibles pour un tiers. Toutefois, au Canada, depuis le 30 novembre 2021, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a mis en place une nouvelle technologie visant à lutter contre les appels mystifiés, appelée STIR/SHAKEN*. Cette dernière permettrait aux différents fournisseurs de services de télécommunication de déterminer la légitimité de l'identité de l'appelant. Le CRTC affirme que les impacts de cette technologie pourraient se faire sentir à condition que « les fournisseurs de services poursuivent la mise à niveau de leurs réseaux sur IP et qu'ils continuent d'offrir des téléphones compatibles à leurs clients » [53].

Hypertrucage (Deepfake)

Relevant d'un processus combinant algorithme et apprentissage profond, **l'hypertrucage permet à un individu de remplacer le visage d'une personne par un autre, sur une vidéo, le tout de façon très réaliste** [39]. Cette technologie, est particulièrement utilisée à des fins pornographiques, touche essentiellement les femmes et représente donc une réelle menace pour les victimes de violence conjugale [39]. En effet, ces images peuvent être utilisées à des fins de sextorsion, pour publication sur des sites pornographiques ou de *revenge porn* et ternir l'image de la victime en les acheminant à son employeur, sa famille et ses amis. Il est également à noter que l'hypertrucage non pornographique en hausse, notamment dans des cas de harcèlement et menace post-séparation [47].

Enregistreur de frappe

L'enregistreur de frappe est un logiciel qui enregistre toutes les interactions effectuées sur un clavier [57]. Bien qu'il s'agisse d'un produit ayant des utilisations complètement légales, par exemple dans le contexte d'un emploi, il peut être utilisé à des fins malveillantes en afin de collecter toutes sortes d'informations telles que les mots de passe, identifiants et noms d'utilisateurs, adresses courriel ou données bancaires. De plus, ces logiciels ont également d'autres fonctionnalités telles que la surveillance par la caméra ou même l'écoute par le contrôle du microphone [58].

La lutte contre l'utilisation des technologies dans les violences conjugales

Dans un contexte de violence conjugale facilitée par les technologies, il est important de rappeler que **le fardeau de l'utilisation sécuritaire des TIC ne devrait pas reposer sur les victimes, mais se concentrer sur les utilisations malveillantes par les ex-partenaires**. En effet, il importe de se soucier des enjeux de revictimisation des victimes, mais également de l'accès sécuritaire aux appareils électroniques. La sécurité des victimes ne doit pas passer par une suppression ou une limitation de l'utilisation des technologies par les victimes. Or, la lutte aux violences facilitées par les technologies est loin d'être simple et il importe donc d'utiliser les moyens disponibles afin de protéger le plus possible les victimes. Il est à noter que dans ce contexte, **les conseils de cybersécurité actuels sont moins propices aux victimes et peuvent même conduire à des effets inverses**.

En effet, la mesure de désactivation des appareils et différents comptes n'améliore pas nécessairement la sécurité des victimes de violence conjugale [59]. En effet, l'effet contraire peut être observé :

- Si le partenaire ne peut rejoindre la victime par le biais de la technologie, il y a une préoccupation que ce dernier tente d'établir un contact en personne.
- Si la victime ne répond pas à son partenaire (ou ex), elle pourrait faire face à des représailles ou une montée de violence.
- La réception de messages, même abusifs, donne un sentiment de contrôle pour certaines victimes, leur permettant de rester informées de l'état psychologique du partenaire. Ainsi, une déconnexion complète peut augmenter l'anxiété de la victime en créant un sentiment d'imprévisibilité.

En matière de solutions technologiques, aucun outil anti-logiciel espion, logiciel permettant de détecter la présence de logiciel espion, ne détecte efficacement les applications de surveillance utilisée par les conjoints violents [46]. L'outil le plus efficace identifié, Anti Spy Mobile, aurait un taux de faux positifs s'élevant à 12 % et signalait des applications légitimes comme Google Chrome en tant que logiciel espion [46].

Mesures et outils à instaurer

Voici quelques recommandations concernant des mesures à instaurer au Québec et au Canada afin de lutter contre le fléau.

Création de campagnes de sensibilisation à plusieurs niveaux

Afin de lutter contre l'utilisation des technologies en contexte de violence conjugale, le gouvernement, les organismes d'applications de la loi ainsi que les organismes communautaires doivent s'unir afin de **lancer plusieurs campagnes de sensibilisation permettant de conscientiser les individus à la problématique ainsi qu'à ces impacts dévastateurs**. L'objectif de la sensibilisation auprès des intervenants serait d'accroître leur compréhension du phénomène ainsi que la nouvelle réalité de leur travail intégrant la protection des données et des appareils lors de l'intervention auprès des victimes de violence conjugale. Il importe également de sensibiliser les victimes et leur cercle de soutien afin de renforcer leur vigilance quant aux utilisations malveillantes des nouvelles technologies.

Formations continues sur l'utilisation des technologies en matière de violence conjugale

Les intervenantes et intervenants en violence conjugale doivent recevoir des formations vulgarisées sur le sujet. Le contenu de ces formations doit non seulement inclure les principes de base en cybersécurité (paramètres de confidentialité, données de localisation, mise à jour des appareils, etc.), mais également les outils et moyens spécifiques utilisés pouvant être utilisés par les conjoints violents. Étant donné les évolutions rapides des technologies, il importe que **ces formations soient offertes de manière continue et soient les plus exhaustives possibles afin que les intervenant.e.s soient en mesure d'intervenir adéquatement**. De plus, les formations devraient inclure une portion pratique ainsi qu'une démonstration en direct afin que les éléments théoriques présentés soient bien compris. Dans la mesure du possible, l'ensemble des intervenantes du milieu devraient suivre ces formations afin que l'offre d'aide offerte en matière de sécurisation des appareils et des données soit constante. Quelques personnes par service pourraient également être nommées comme « Champion technologie » afin de répondre aux questions de leur collègue en cas de doute ou outiller les nouveaux intervenants qui n'auraient pas nécessairement le temps au préalable de suivre les formations avant de mener leurs interventions. En ce sens, la formation continue serait un excellent moyen d'outiller les intervenants afin de leur permettre d'intervenir le plus efficacement possible face à une situation de cyberviolence, de même que diffuser leurs connaissances aux femmes victimes et ainsi favoriser l'autonomisation des victimes.

Mise en place d'un groupe de travail spécialisé sur l'utilisation des technologies dans les violences faites aux femmes

Au niveau gouvernemental, **les ministères concernés devraient mettre en place un groupe de travail incluant des chercheurs et des professionnels dans plusieurs domaines tels que la cybersécurité (ou l'informatique de manière générale), la psychologie, le droit, le travail social, la victimologie et la criminologie afin d'élaborer des outils concrets pour lutter contre l'utilisation des technologies dans les violences faites aux femmes**. Les recherches de ce groupe spécialisé pourraient servir à réfléchir à une façon d'instaurer un programme de protection uniformisé dans toutes les maisons d'hébergement. Par exemple, le gouvernement pourrait fournir aux maisons un protocole de base rigoureux à suivre et régulièrement mis à jour afin de prévenir et de contrôler les cyberviolences.

Création de dispositifs identifiant les intrusions technologiques malveillantes

Il serait également pertinent de **créer des applications ou dispositifs plus efficaces permettant de tester les appareils électroniques des victimes afin de détecter de potentiels logiciels malveillants**. D'ailleurs, le tribunal judiciaire de Paris a lancé « Veriphone » un dispositif disposant d'un Code QR qui permet la vérification d'une présence de logiciels espions sur un appareil [60]. Ce dernier est gratuit et le rapport d'analyse produit peut être ajouté à un dossier judiciaire ou une plainte en cas d'infection [60]. En ce sens, il serait intéressant d'élaborer ce genre d'outil au Québec et au Canada, disponible dans les services de police, les tribunaux et les services d'aide aux victimes afin de mieux les protéger contre les cyberviolences.

Ressources existantes

La boîte à outils du Centre de documentation sur l'éducation des adultes et la condition féminine (CDÉACF)

Créée dans le cadre du projet « Comptes et appareils connectés en contexte de violence conjugale : mieux comprendre les technologies pour prévenir les risques reliés à la localisation et à l'utilisation des comptes en ligne », la **boîte à outils du CDÉACF** est une ressource rassemblant différents matériels de sensibilisation (en français) permettant aux victimes de s'informer sur des sujets tels que la localisation, les comptes partagés et les appareils connectés. On y retrouve également des capsules d'animation, différentes affiches et brochures thématiques, des jeux interactifs ainsi que de l'information sur différentes ressources en ligne disponibles pour les victimes de violence conjugale.

Les boîtes à outils du National Network to End Domestic Violence (disponible en anglais seulement)

Le NNEDV a lancé le projet intitulé « **Safety Net** » afin d'offrir des ressources informatives aux victimes et intervenantes en violences conjugales sur l'utilisation des technologies. Ces ressources sont regroupées sous six boîtes à outils. Parmi celles-ci, la boîte du survivant offre des informations précises et des conseils sur diverses thématiques telles que la sécurité et la technologie de base, les logiciels espioons (qu'est-ce qu'ils sont, comment fonctionnent-ils, comment s'en débarrasser, etc.), la confidentialité des données en ligne. La boîte à outils des services aux victimes présente du contenu tel que l'évaluation des abus technologiques ainsi que plusieurs informations techniques et plus pointues sur la sécurité des données et des appareils. Bien que l'information originale soit en anglais et en espagnol, le traducteur de navigateur chrome peut-être utilisé pour présenter l'information dans un autre langage.

Documentaire du Technology Safety for Survivors of Domestic and Sexual Violence

Cet **outil documentaire** offre non seulement des informations explicatives sur l'utilisation de la technologie en contexte de violence conjugale ainsi que des outils malveillants utilisés par les conjoints violents, mais également un guide permettant d'augmenter son niveau de sécurité lors de l'utilisation de la technologie. Plus particulièrement, l'outil offre des instructions détaillées sur la façon dont gérer ses paramètres de confidentialité sur plusieurs plateformes telles que Facebook, Instagram, Snapchat, Twitter ainsi que directement sur les téléphones cellulaires de type iPhone et Android. Finalement, le documentaire offre des conseils sur la gestion sécuritaire des mots de passe. Bien que l'information originale soit en anglais, le traducteur de navigateur chrome peut-être utilisé pour présenter l'information dans un autre langage.

Références

[1] National Network To End Domestic Violence (NNEDV). (S.D). *Safety Net Project*. **[lien]**

[2] Sugiura, L., Blackbourn, D., Button, M., Hawkins, C., Tapley, J., Frederick, B. et coll.. (2021). Computer Misuse as a Facilitator of Domestic Amuse. *School of Criminology and Criminal Justice. University of Kent*. **[lien]**

[3] Institut national de santé publique du Québec (INSPQ).(2018). *Cyberviolences dans les relations intimes. Trousse média sur la violence conjugale*. **[lien]**

[4] Fernet, M., Lapierre, A., Hébert, M., Cousineau, M.-M. (2019). A Systematic Review of Literature on Cyber Intimate Partner Victimization in Adolescent Girls and Women. *Journal of Computers in Human Behavior,* 100(*Issue C*), 11-25. **[lien]**

[5] Storey, J. E., Pina, A., Duggan, M., et Franqueira, V. N. L. (2021). *Technology-Facilitated Intimate Partner Violence: A multidisciplinary examination of prevalence, methods used by perpetrators and the impact of COVID-19*. Home Office. **[lien]**

[6] APC Women's Networking Support Programme (WNSP). (2011). *Comment la technologie sert à perpétrer la violence faite aux femmes — et à la combattre*. Association for Progressive Communications. **[lien]**

[7] Gauvreau, C. (2022). *Prévention des cyberviolences*. Actualités UQAM. **[lien]**

[8] Slupska, J. etTanczer, L. M. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. Dans Bailey, J., Flynn, A. et Henry, N. (dir.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies In Digital Crime, Technology and Social Harms)* (p. 663-688),. Bingley: Emerald Publishing Limited. **[lien]**

[9] Think Social Tech, Snook, & SafeLives. (2019). *Tech vs abuse: Research findings 2019* (p. 1–39). Comic Relief, The Clothworkers' Foundation, and Esmée Fairbairn Foundation.

[10] Women's Aid. (2018). *Online and digital abuse*. Women's Aid. **[lien]**

[11] Woodlock, D., McKenzie, M., Western D. et Harris, B. (2020). Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control. *Australian Social Work*, *73*(3), 368-380. **[lien]**

[12] Tanczer, L. M., Parkin, S., Danezis, G. et Patel, T. (2018). *The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT)*. London Global University. **[lien]**

[13] Freed, D. Palmer,J.Minchala,D. Levy, K. , Ristenpart,T. et Dell, N. (2018). A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, Paper 667, 1–13. **[lien]**

[14] Bernier, A. (2016). *L'utilisation des TIC à des fins de harcèlement criminel en situation de violence conjugale : la théorie des opportunités et des activités routinières de Cohen et Felson (1978)*. (Mémoire de maîtrise, Université de Montréal). **[lien]**

[15] Landry, A. (2022, 4 décembre). La technologie, l'arme invisible pointée sur les victimes de violence conjugale. *Radio Canada*. **[lien]**
[16] West, J. (2014). *Cyberviolence against Women. Battered Women's Support Services*. University of British Columbia. **[lien]**
[17] Hango, D (2016). *Regards sur la société canadienne : La cyberintimidation et le cyberharcèlement chez les utilisateurs d'Internet âgés de 15 à 29 ans au Canada*. Statistique Canada. **[lien]**
[18] Council of Europe. (S.D). *Cyberviolence : Cyberviolence at a Glance : Types of cyberviolence*. **[lien]**
[19] Roger, E. (2020). *Vers une loi interdisant l'espionnage dans le couple : « Ça amène très vite à la psychose ». Europe 1*. **[lien]**
[20] Pettinari, D. (2000). *Cyberstalking investigation and prevention. Standard Operating Procedures*. Pueblo High-Tech Crimes Unit Investigative and Technical Protocols. **[lien]**
[21] Benedictis,T., Jaffe, J. et Segal, J. (2006). Domestic Violence and Abuse: Types, Signs, Symptoms, Causes, and Effects. *The American Academy of Experts in Traumatic Stress*. **[lien]**
[22] Stevens, R.C. J. et Arief, B. (2021). Cyberstalking can be defined as ''the use of the Internet, e-mail, or other electronic communications devices to stalk another person''. *Cyberpsychology, behavior and social networking, 24*(6). **[lien]**
[23] Finley, J (2022). 'Uptick' in women stalked by new technology in Nashville. *WSMV 4*. **[lien]**
[24] Fondation Marie-Vincent (2019). *La cyberviolence sexuelle*. **[lien]**
[25] La Presse canadienne. (2022, 6 août). Les cas de sextorsion ont grimpé en flèche au Canada. *Radio-Canada*. **[lien]**
[26] Al-Alosi, H. (2017). Cyber-violence : digital abuse in the context of domestic violence. *University Of New South Wales Law Journal*, *40*(4), 1573-1603. **[lien]**
[27] McGlynn, C. et Rackley, E. (2016). Not 'Revenge Porn,' But Abuse: Let's Call It Image-Based Sexual Abuse. *Inherently Human: Critical Perspectives on Law, Gender & Sexuality*, *41*.
[28] Patchin, J. W. et Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse*, *32*(1), 30–54. **[lien]**
[29] Radio-Canada. (2018, 23 mars). Échange massif de photos pornographiques : des victimes témoignent. **[lien]**
[30] National Network to End Domestic Violence (NNEDV). (2014). A Glimpse From the Field: How Abusers Are Misusing Technology. *Safety Net Technology Safety Survey*. **[lien]**
[31] Tillous, M. (2020). *L'usage des outils de géolocalisation au sein du couple :contrôle spatial et violences conjugales*. Université de Paris. **[lien]**
[32] Shahani, A. (2014, 15 septembre). Smartphones Are Used To Stalk, Control Domestic Abuse Victims. *NPR*. **[lien]**

[33] Henry, N., Vasil, F., Flynn A., Kellard, K. et Mortreux, C. (2021). Technology-Facilitated Domestic Violence Against Immigrant and Refugee Women: A Qualitative Study. *Journal of Interpersonal Violence*, 1–27. **[lien]**
[34] Chin, M., Song, V. (2022, 1er mars). *AirTags are dangerous — here's how Apple could fix them*. *The Verge*. **[lien]**
[35] Nelson, T. (2021, 10 novembre). Geofencing: What It Is and How It Works. *Lifewire*. **[lien]**
[36] Saleh, I. (2018). *Internet des Objets (IdO) : Concepts, Enjeux, Défis et Perspectives*. Université de Paris 8. **[lien]**
[37] Madakam, S., Ramaswamy, R. et Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, *3*, 164-173. **[lien]**
[38] Lo, M. (2021). A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law. *California Law Review*. *109*(277). **[lien]**
[39] Van Der Wilk, A. (2021). Protecting women and girls from violence in the digital age: The relevance of the Istanbul Convention and the Budapest Convention on cybercrime addressing online and technology-facilitated violence against women. *Council of Europe*. **[lien]**
[40] IHS Markit. (2017). *The Internet of Things: A movement, not a market*. Englewood, United States: IHS Markit.
[41] Janes, B., Crawford, H. et OConnor,T .(2020). Never Ending Story: Authentication and Access Control Design Flaws in Shared IoT Devices. *2020 IEEE Security and Privacy Workshops (SPW)*, 104-109. **[lien]**
[42.] Parkin, S. , Patel, T. , Lopez-Neira, I. et Tanczer, L. M. (2019). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. Dans M. Carvalho , W. Pieters et E. Stobert (dir.), *Proceedings of the new security paradigms workshop* (p. 1–15). New York, NY: Association for Computing Machinery (ACM). **[lien]**
[43] Riley, A. (2020, 11 mai). Comment vos appareils domestiques intelligents peuvent se retourner contre vous. *BBC Future*. **[lien]**
[44] Bowels, N. (2018, 23 juin). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *NY Times*. **[lien]**
[45] Braithwaite, P. (2018, 22 juillet). Smart home tech is being turned into a tool for domestic abuse. *Wired*. **[lien]**
[46] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D. et coll. (2018). The Spyware Used in Intimate Partner Violence. *2018 IEEE Symposium on Security and Privacy (SP),* 441-458. **[lien]**
[47] New York State Office for the Prevention of Domestic Violence. (S.D). *Technology Safety for Survivors of Domestic and Sexual Violence*. **[lien]**
[48] Southworth, C., Finn, J., Dawson, S., Fraser, C. et Tucker, S. (2007). Intimate Partner Violence, Technology, and Stalking. *Violence Against Women*, *13*(8), 842- 856.

[49] Singh, A. (2015). Research on Hacking Team and Finfisher highlighted in Motherboard. *Citizen Lab*. **[lien]**
[50] Harkin, D., Molnar, A. et Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture, 16*(1), 33-60. **[lien]**
[51] Maiorca, D. (2021, 12 juillet). *Qu'est-ce que Cydia sur mon iPhone et qu'est-ce que cela signifie pour ma sécurité ? Makeuseof*. **[lien]**
[52] Dumont, G. (2019, 24 mars). Des femmes victimes de violence conjugale traquées par des moyens technologiques. *Radio-Canada*. **[lien]**
[53] Conseil de la radiodiffusion et des télécommunications canadiennes. (2021). Les Canadiens bénéficieront d'une nouvelle technologie d'identification de l'appelant pour lutter contre les appels mystifiés. *Gouvernement du Canada*. **[lien]**
[54] Federal Communications Commission. (2022). *Consumer Guides: Caller ID Spoofing*. **[lien]**
[55] Sneeringer, G. (2015). Contact That Can Kill: Orders of Protection, Caller ID Spoofing and Domestic Violence. *90 Chi.-Kent L. Rev.,* 1157. **[lien]**
[56] Women's Law.org. (2018). Abuse Using Technology: What are some ways an abuser could use spoofing technology? *National Network For Domestic Violence*. **[lien]**
[57] Stouffer, C. (2021). Keyloggers 101: A definition + keystroke logging detection methods. *Norton*. **[lien]**
[58] Malwarebytes. (S.D). Keylogger : What is a keylogger ? *Malwarebytes*. **[lien]**
[59] Woodlock, D. (2017). The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*, *23*(5), 584-602.
[60] CNEWS. (2022). Paris : Qu'est-ce que le dispositif « Veriphone » mis en place par le tribunal judiciaire pour lutter contre le harcèlement. *CNEWS*. **[lien]**