LES3SEX*

Sexe. Sexualité. Sexologie

COMPRENDRE LA SEXTORSION POUR MIEUX LUTTER: RAPPORT DE RECHERCHE DOCUMENTAIRE, DÉFINITION ÉLARGIE DU PHÉNOMÈNE ET RECOMMANDATIONS SOMMAIRES

PAR

FLAVIE COLLIN

ZOE YARYMOWICH

PAMELA PLOURDE

RÉVISION

MARIANNE COUTURE-COSSETTE

MAGALI GUILBAULT-FITZBAY

MYLÈNE DE REPENTIGNY-CORBEIL

MARIANE GILBERT

JUILLET 2022

Patrimoine canadien

Canadian Heritage

TABLE DES MATIÈRES

LISTE DES FIGURES

INTRODUCTION

Les technologies de l'information et de la communication (TIC) ont modifié les façons dont les individus entrent en relation, s'informent, communiquent et se présentent (Macilotti, 2019). Grâce à la technologie, les individus peuvent désormais entrer en contact facilement et rapidement, et ce, bien au-delà des frontières physiques et temporelles (Koch et Miles, 2021). La communication en ligne offre également aux internautes l'opportunité de façonner leur image et de moduler leur identité : il devient alors possible de se dévoiler sans aucun filtre ou, au contraire, de dissimuler ou modifier certains aspects de sa vie personnelle (Bouchard et Lussier, 2006). Selon certain.e.s auteur.e.s, les interactions numériques favorisent la création d'un lien de confiance rapide entre les interlocuteurs et les interlocutrices (Close *et al*., 2004) et diminuent la peur du jugement social (Bouchard et Lussier, 2006). Le numérique permettrait également aux personnes marginalisées, notamment sur la base de leur identité de genre, de leur couleur de peau, de leur origine ethnoculturelle et/ou de leur orientation sexuelle, de contrer l'invisibilisation de leur identité et d'élargir leurs cercles sociaux (Bouchard et Lussier, 2006).

Cependant, bien que les avancées technologiques comportent de nombreux avantages et favorisent l'avènement de certains changements sociaux positifs, elles comportent également certains risques. En effet, la criminalité évolue parallèlement au développement des TIC (Li, 2017). Par exemple, bien que les médias sociaux soient utiles pour maintenir les contacts avec les proches, ils favorisent toutefois un partage accru d'informations personnelles sensibles et confidentielles (Geldenhuys, 2016). De plus, la démocratisation des appareils portables munis de caméra et la popularité des applications centrées sur le partage d'images vont de pair avec l'importance accordée aux images numériques, sans oublier que l'omniprésence des réseaux sociaux et l'affinement des technologies favorisent l'émergence de nouvelles pratiques sexuelles (Holt et Ligget, 2020). Cette réalité s'accompagne de nouvelles manifestations de violences à caractère sexuel. Il est effectivement de plus en plus fréquent que les images intimes soient utilisées pour porter atteinte à l'intégrité d'une personne. L'utilisation malveillante des images intimes est un phénomène complexe, et l'omniprésence des technologies contribue à l'occurrence de violence basée sur l'image (Citron et Franks, 2014; Henry et Powell, 2015; McGlynn, Rackley et Houghton, 2017). Ce phénomène est d'autant plus notable depuis le début de la pandémie de la COVID-19, puisque le temps passé en ligne a considérablement augmenté, que ce soit pour des raisons personnelles, professionnelles ou scolaires. Considérant que les contacts physiques avec autrui en temps de pandémie sont devenus limités voire absents, la sexualité en ligne s'est particulièrement popularisée. À ce titre, Nelson et ses collègues (2020) observent une augmentation de la masturbation, de la sexualité en ligne et de la consommation de pornographie chez les adolescent.e.s de la diversité sexuelle et de genre. Aussi, certain.e.s auteur.e.s notent une augmentation des téléchargements d'applications de rencontre et des publications érotiques sur les médias sociaux en temps de pandémie (Lehmiller *et al*., 2021).

Face à l'avènement des nouvelles technologies et à leur popularité grandissante, il s'avère impératif de documenter les diverses formes de violences à caractère sexuel en ligne, tout particulièrement la sextorsion, qui fait l'objet du présent rapport. Au cours des dernières années, ce crime à caractère sexuel a attiré l'attention du milieu de la recherche ainsi que des instances gouvernementales. Cependant, malgré l'intérêt grandissant de la communauté scientifique à l'égard de la sextorsion, les données probantes à ce sujet demeurent limitées. Le

présent rapport propose ainsi une définition élargie du phénomène de la sextorsion, un bref portrait de sa prévalence, ses liens avec les nouvelles technologies, ses conséquences sur les personnes qui en sont victimes ainsi que les divers recours auxquels ces dernières ont droit. La recherche exploratoire se base sur des données empiriques, des articles journalistiques, des textes théoriques ainsi que des programmes de sensibilisation et de prévention créés par divers organismes ou instances gouvernementales. À la lumière des lacunes identifiées lors de notre recherche exploratoire, diverses recommandations et pistes de solution sont proposées afin de lutter contre la sextorsion.

1. LA SEXTORSION : UN CRIME SEXUEL AUX APELLATIONS MULTIPLES

1.1. Définitions et formes de sextorsion

La sextorsion est un mot-valise constitué des termes « sexe » et « extorsion » et recoupe plusieurs phénomènes de violences à caractère sexuel prenant place principalement en ligne. Dans la littérature scientifique comme dans les médias, la sextorsion est souvent considérée en tant que forme de cyberintimidation, de chantage, d'extorsion, d'abus de pouvoir, de fraude ou d'exploitation sexuelle. D'autres termes sont également utilisés pour parler du phénomène tels que l'agression sexuelle à distance, la cyberagression sexuelle, le chantage par webcam et la corruption sexuelle. Le plus souvent, la sextorsion est définie en tant que menaces de partage d'images intimes dans le but de contraindre une personne à envoyer davantage d'images sexuellement explicites ou à offrir des faveurs sexuelles (Henry, Flynn et Powell, 2018). La sextorsion est également définie par certain.e.s auteur.e.s comme l'usage de la tromperie afin de porter une personne à se dévêtir devant la caméra, et ce, dans le but de capturer des images sexuellement explicites qui seront ultérieurement utilisées comme levier pour réclamer de l'argent (McGlynn *et al*., 2017; Henry, Flynn et Powell, 2018; Paat et Markham, 2021).

Bien que plusieurs définitions de la sextorsion circulent, celles-ci rendent rarement compte de la complexité du phénomène. En ce qui a trait à la nature des menaces, il est question de sextorsion lorsqu'une menace de partager du contenu sexuellement explicite est proférée. Toutefois, tel que le proposent Grubb et ses collègues (2019), il est nécessaire de considérer le chantage visant le partage d'informations de nature sexuellement explicite ou compromettante dans le cas où la personne ciblée refuse de se plier aux demandes de la personne qui exerce la sextorsion. En ce qui concerne le contexte dans lequel la sextorsion se déroule, les définitions et les études qui circulent renvoient généralement à la cybersextorsion, qui prend place sur les réseaux sociaux, les applications de messagerie instantanée et de conversation vidéo ou sur les plateformes de jeux vidéo (Wittes *et al*., 2016; Wolak et Finkelhor, 2016). Cependant, bien que plusieurs auteur.e.s considèrent que la sextorsion a nécessairement une composante technologique, cette dernière se manifeste également dans le monde physique. À ce sujet, Murr (2006) propose une itération de la sextorsion qui prend place entièrement hors ligne, la *supervisory sextorsion*, qui a lieu entre autres lorsqu'un.e supérieur.e réclame des faveurs de nature sexuelle sous la menace de destitution ou de tout autre dommage lié à l'emploi. Wittes, Poplin, Jurecic et Spera (2016) considèrent aussi les situations où des personnes sont maintenues de force dans une situation d'exploitation sexuelle par un proxénète les menaçant de partager des informations ou du contenu compromettant. Finalement, il existe des situations où la sextorsion sert de moyen de corruption pour réclamer des faveurs sexuelles en échange d'accès à des services publics tels que l'éducation, des services de santé ou des biens de base (Feigenblatt, 2020). En 2010, le National Post rapportait le cas d'un agent d'immigration qui

refusait d'octroyer un statut de réfugié à une femme sud-coréenne si cette dernière n'acceptait pas de lui procurer certaines faveurs sexuelles (Kari, 2010). Somme toute, il existe très peu d'études empiriques faisant état de formes de sextorsion qui ne mobilisent aucune composante technologique.

Force est d'admettre que la sextorsion est un phénomène complexe qui prend plusieurs formes et se déploie dans différents contextes. Par conséquent, il nous est impossible d'aborder l'ensemble des manifestations du phénomène. Néanmoins, il est possible d'affirmer que la sextorsion représente, dans tous les cas, une forme de chantage de nature sexuelle (Vasiu et Vasiu, 2020).

1.2. La sextorsion et ses notions connexes : déblayage conceptuel

La sextorsion se manifeste souvent de pair avec d'autres types de violences basées sur l'image, si bien que celle-ci est fréquemment conceptualisée uniquement en tant que forme de cyberviolence à caractère sexuel. Selon certain.e.s auteur.e.s, un geste de violence à caractère sexuel facilité par la technologie (VCSFT) est commis lorsqu'une personne instrumentalise la technologie afin de poser un geste de violence à caractère sexuel dans le monde virtuel ou physique (Henry et Powell, 2018). Henry et Powell (2015; 2019) ont identifié quatre manifestations de VCSFT, soit le cyberharcèlement sexuel, la violence à caractère sexuel basée sur l'image, l'agression et la coercition sexuelles et le harcèlement sexuel basé sur le genre et la sexualité. Tel que mentionné précédemment, dans un contexte de sextorsion, les images intimes, obtenues de façon consensuelle ou non, sont fréquemment utilisées comme levier pour faire chanter les victimes. Cette utilisation malveillante des images intimes est présente dans chacune des formes de VCSFT mais ne peut rendre compte de l'ensemble des actes de sextorsion, considérant qu'un nombre élevé d'entre eux peuvent se produire hors ligne. Le concept de VCSFT occulte ainsi les manifestations de la sextorsion qui n'ont pas de composante technologique.

Connexe à la VCSFT, la violence à caractère sexuel basée sur l'image (VCSBI) est aussi étroitement liée à la sextorsion. Considérée par certain.e.s auteur.e.s comme une forme de VCSFT (Henry, Flynn et Powell, 2018), le concept de VCSBI, proposé par McGlynn et Rackley (2017), s'inspire du concept de continuum de violence à caractère sexuel de Kelly (1988). Ce continuum expose une série d'actes sexuellement abusifs, allant du *catcalling* à l'agression sexuelle. Henry et ses collègues (2018) identifient trois types de VCSBI, soit la création non consensuelle d'images intimes, le partage non consensuel d'images intimes (PNCII) ainsi que la menace de partage d'images intimes. Ce troisième et dernier type de VCSBI ferait, selon Henry et ses collègues (2018), référence à des actes de sextorsion. Bien qu'il s'agisse d'un concept englobant plusieurs actes sexuellement abusifs, le VCSBI ne permet pas de faire de distinction entre la menace de publier une image sans consentement et la mise à exécution de cette menace. La VCSBI laisse également de côté les cas d'utilisation d'informations compromettantes pour contrôler des victimes (Henry, Flynn et Powell, 2018). Par exemple, en octobre 2021, le plus grand site de rencontre LGBTQ+ israélien a été la cible d'une cyberattaque. Les pirates informatiques réclamaient une rançon sous menace de publier les données complètes des usagères et usagers, telles que leur identité, leur statut séropositif et leur orientation sexuelle (Lanney, 2021).

La sextorsion est aussi fréquemment confondue avec le PNCII, communément appelé *revenge porn*. Tout comme la sextorsion, le PNCII fait l'objet de nombreuses définitions. Défini par Henry et ses collègues (2018) en tant qu'acte de diffusion d'images et/ou de vidéos

intimes sans le consentement de la personne les ayant produites, le PNCII est parfois présenté comme une forme de cyberintimidation, de cyberviolence, de cyberhumiliation, de cyberharcèlement ou comme un outil de contrôle (Dilmac, 2017). Plusieurs termes sont utilisés afin de faire référence au PNCII, tels que le sextage secondaire (Fortin et Desfachelles, 2019), la pornographie non consensuelle (Hill, 2015), la pornographie involontaire (McGlynn *et al*., 2017) ou encore la *revenge porn* (Citron et Franks, 2014).

L'expression« *revenge porn* » est la plus fréquemment mobilisée au sein des médias et des discours populaires lorsqu'il est question de partage non consensuel d'images intimes. Cependant, l'utilisation de cette formule est de plus en plus critiquée par le milieu de la recherche et les milieux féministes puisque l'accent repose davantage sur la nature du contenu que sur le caractère abusif du comportement. Le contenu sexuel partagé sans consentement ne peut être considéré comme une forme de pornographie, il apparaît donc nécessaire de trouver un terme illustrant le caractère abusif de l'acte (Henry et Flynn, 2019; McGlynn *et al*., 2017). Qui plus est, l'expression « *revenge porn* » ne rend pas justice à l'ensemble des motivations qui alimentent le geste. En effet, outre la vengeance, l'individu perpétrant le PNCII peut être motivé par des raisons monétaires, sociales, de divertissement, de domination, de gratification sexuelle ou encore, ne présenter aucune motivation apparente (DeKeseredy et Schwartz, 2016; Henry et Flynn, 2019; Henry et Powell, 2015a). Malgré le fait que la sextorsion et le PNCII soient interreliés et que leur occurrence puisse coïncider, les deux phénomènes ne sont pas interchangeables. Bien que la sextorsion comporte généralement une composante numérique, tel que mentionné précédemment, elle n'est pas toujours facilitée par la technologie, à la différence du partage non consensuel d'images intimes dont les évènements dans le monde physique relèvent de l'exception (Acar, 2016, dans O'Malley et Holt, 2022; Carlton, 2019).

Enfin, l'extorsion est inscrite au code criminel, et se voit plus facilement condamnée. Du point de vue juridique, lorsqu'il est question d'extorsion, il n'est pas nécessaire que la victime cède aux désirs de l'extorqueur ou de l'extorqueuse pour qu'il y ait infraction, c'est-à-dire que les menaces n'ont pas à être mises à exécution pour qu'il s'agisse d'un acte d'extorsion. En effet, dans le Code criminel canadien (1985), on peut lire :

> « Commet une extorsion quiconque, sans justification ou excuse raisonnable et avec l'intention d'obtenir quelque chose, par menaces, accusations ou violence, induit ou tente d'induire une personne, que ce soit ou non la personne menacée ou accusée, ou celle contre qui la violence est exercée, à accomplir ou à faire accomplir quelque chose. » (art. 346(1)).

En considérant l'article 346(1) du Code criminel canadien, **il serait donc question de sextorsion lorsque l'acte d'extorsion comporte une menace de nature sexuelle ou une menace de porter atteinte à la santé sexuelle ou aux droits sexuels[1] d'une**

[1] Les 3 sex* définit les droits sexuels comme suit :

1. Droit de s'épanouir, de prendre plaisir et de se développer sexuellement dans la reconnaissance de son agentivité sexuelle et en absence de contraintes, et ce, pour l'ensemble des réflexions, choix et actions concernant sa sexualité.
2. Droit à une éducation et à de l'information récente, accessible, fiable, valide et de qualité vis-à-vis l'ensemble des aspects politiques, juridiques, sociologiques, psychologiques et médicaux de la sexualité.
3. Droit à l'égalité et à la dignité autant socialement, politiquement, juridiquement que médicalement, et ce, peu importe l'identité de genre, le sexe, l'orientation sexuelle et l'expression de genre que toute personne peut définir librement.

personne, que ce soit au niveau du moyen utilisé pour faire chanter la victime ou de la nature de ce que l'on tente de lui soutirer. La sextorsion s'inscrit dès lors dans le spectre des violences à caractère sexuel.

1.3. Limites des définitions existantes

Tel qu'illustré au sein de la précédente section, il n'y a pas de consensus sur ce que constitue un acte de sextorsion. Dans la recherche scientifique comme dans les médias, l'usage du terme réfère plutôt à de la cybersextorsion. La majorité des données sur la sextorsion proviennent effectivement d'études sur la VCSBI qui mobilisent une multitude de définitions, d'instruments de mesure variés et une variété de concepts (Carlton, 2019; Henry et Powell, 2018; Henry et Flynn, 2019). Très peu d'études empiriques portent spécifiquement et exclusivement sur le sujet. La majorité des connaissances sur le phénomène proviendrait effectivement de sources journalistiques (McGlynn *et al*., 2017), limitant la généralisation des résultats.

1.3.2 Au-delà de l'utilisation malveillante des images intimes

Les définitions courantes de la sextorsion, notamment celles relayées dans les médias et au sein des campagnes de sensibilisation gouvernementales, tendent à se focaliser sur l'utilisation malveillante d'images intimes. Toutefois, il est important de porter attention aux incidents où ce sont des informations confidentielles de nature sexuelle (plutôt que du contenu sous la forme d'images) qui sous-tendent le chantage (Grubb *et al.*, 2019). Un sextorqueur ou une sextorqueuse pourrait, par exemple, menacer de révéler le statut séropositif, les infidélités ou l'orientation sexuelle d'une personne qui refuse de se plier à certaines demandes (Lanney, 2021). Encore une fois, il est important de préciser que le but du chantage ne renvoie pas exclusivement à l'obtention d'images intimes. En effet, le sextorqueur ou la sextorqueuse pourrait aussi chercher à obtenir des faveurs sexuelles ou de l'argent, à contraindre une personne à poursuivre une relation, ou encore, obliger quelqu'un à poser des gestes criminels pour porter atteinte à sa réputation ou pour lui retirer tout autre chose, notamment un gain politique. De plus, il importe de considérer comme de la sextorsion les évènements qui n'incluent pas la présence de menaces, mais où une personne a recours à de la tromperie pour obtenir du matériel sexuellement explicite, par exemple, en ayant recours à des tactiques de fraude romantique ou de *catfishing*. Dans certains cas, le passage à l'acte est motivé par simple désir de gratification sociale et sexuelle, d'ascension au sein d'un groupe ou bien par désir de contrôle ou de manipulation (Vasiu et Vasiu, 2020; Wolak et Finkhelor, 2016).

1.3.3 La provenance du contenu

Bien que la manipulation et la tromperie constituent des méthodes particulièrement utilisées par les personnes qui sextorquent afin d'obtenir du contenu sexuellement explicite – méthodes abondamment représentées dans les médias et la littérature scientifique – il existe une foule d'autres moyens pour soutirer du matériel à caractère sexuel. Dans certains cas, le matériel peut d'abord avoir été partagé de manière consensuelle, par exemple dans le cadre d'une relation

4. Droit à la sécurité et à l'inclusion pour l'ensemble des composantes sexuelles et relationnelles dans le respect et la protection de l'intégrité psychologique et physique, et ce, en l'absence de discrimination ou de violence.
5. Droit de bénéficier des avancées scientifiques, des progrès techniques, et de l'accès adapté, gratuit, confidentiel aux soins, services, traitements et produits de qualité en santé sexuelle et reproductive.

intime. Il peut également avoir été obtenu de manière illégale par l'entremise de techniques d'ingénierie sociale telles que l'hameçonnage, les maliciels ou tout autre moyen informatique permettant d'accéder illégalement à du contenu. Le contenu intime peut également provenir de sites dédiés à la *revenge porn* ou avoir été obtenu au sein d'une chaîne de partage, par exemple dans une conversation de groupe dédiée au partage d'images intimes non consensuelles.

Au-delà des images et du contenu intimes obtenus illégalement, il importe d'intégrer dans notre conceptualisation de la sextorsion le contenu créé de manière non consensuelle, notamment par le vidéovoyeurisme, le *upskirting*, le *downblousing* ou l'enregistrement non consenti d'actes sexuels. Le phénomène de création non consensuelle d'images intimes est d'autant plus répandu grâce à l'accès gratuit et répandu aux outils de création de *deepfakes*. En effet, les avancées technologiques, notamment en termes d'intelligence artificielle, permettent facilement et sans connaissances informatiques avancées de sexualiser une image ou d'en créer de nouvelles (voir encadré ci-dessous sur les *deepfakes*). Bien qu'il existe une multitude de méthodes afin d'obtenir du contenu sexuellement explicite, il semble que les principales stratégies visant à commettre des actes de sextorsion soient la tromperie (fraude romantique, *catfishing*, *e-whoring*), le piratage informatique et la violence interpersonnelle (Kelley, 2019)

***Deepfakes* pornographiques : un fléau grandissant, mais négligé[2]**

Par Gabrielle Gendron, coordonnatrice à l'Observatoire des conflits multidimensionnels de la Chaire de recherche Raoul-Dandurand en Études stratégiques et diplomatiques

Faut-il encore le voir pour le croire ? Face aux récents progrès de l'intelligence artificielle, la question se pose. En effet, les avancées en matière de synthèse d'images humaines permettent désormais au grand public de superposer des images et des vidéos existantes sur des vidéos sources, pour créer ce qui est communément appelé des « *deepfakes* » (ou hypertrucage).

Les *deepfakes* sont des vidéos hyperréalistes qui font appel à l'intelligence artificielle pour dépeindre des personnes disant et faisant des choses qui n'ont jamais eu lieu. Le mot « *deep* » provient des méthodes d'apprentissage automatique du *deep learning* (ou apprentissage profond), qui consiste en des réseaux de neurones artificiels visant à analyser de vastes ensembles d'échantillons de données et ainsi apprendre à imiter les expressions faciales, les manières, la voix et les inflexions d'une personne. Plus précisément, ce processus consiste à introduire des séquences vidéo de deux personnes dans un algorithme d'apprentissage profond pour l'entraîner à échanger les visages.

Fruit d'une longue évolution

La manipulation du contenu numérique n'est pas un phénomène nouveau. En effet, c'est en 1997 que le premier *deepfake* voit le jour. Programmé par trois chercheurs et chercheuses états-unien.ne.s, le dispositif Video Rewrite était le premier système à

[2] Ce texte est d'abord paru le 29 mars 2022 en tant que Chronique des nouvelles conflictualités écrite dans le cadre du partenariat entre Les 3 sex* et la Chaire de recherche Raoul-Dandurand en études stratégiques et diplomatiques.

automatiser entièrement ce type de réanimation faciale. Inoffensif à ce stade, le programme était destiné à des applications de doublage de films, permettant de modifier la séquence vidéo pour synchroniser les mouvements des lèvres des acteurs et actrices avec une nouvelle bande sonore. Le terme « *deepfake* » est tiré du nom d'un utilisateur de Reddit qui, en 2017, commence à utiliser des outils d'intelligence artificielle standard pour coller le visage de célébrités sur des vidéos pornographiques.

Le *deepfake* connaît alors une croissance rapide en ligne : en 2019, une étude publiée par la firme Deeptrace recensait 14 678 vidéos de *deepfakes* sur Internet. Un an plus tard, Sentinel AI publiait un rapport sur l'état des *deepfakes* et recensait 145 277 vidéos de ce type sur Internet, soit une multiplication par dix en l'espace d'une année. Bien que la pornographie reste l'usage le plus fréquent de technologie *deepfake*, celle-ci commence aussi à produire un impact important sur la sphère politique ainsi que sur le paysage de la cybersécurité, renforçant notamment les cybermenaces traditionnelles et offrant des vecteurs d'attaques entièrement nouveaux.

De faibles barrières à l'entrée

La création de *deepfakes* est désormais un processus non dispendieux et relativement facile à déployer. En effet, grâce aux réseaux sociaux, il existe sur Internet une grande quantité d'images et de vidéos de visages qui sont accessibles au public et qui peuvent être utilisées comme données d'apprentissage. La puissance de calcul nécessaire pour faire fonctionner ces réseaux est peu coûteuse et facilement disponible grâce à l'informatique en nuage. Cette faible barrière à l'entrée fait donc des *deepfakes* une arme puissante pour quiconque a accès à Internet et dispose d'outils de création adéquats.

Les algorithmes utilisés pour la création de *deepfakes* peuvent visionner des milliers de photos d'une personne et produire un nouveau portrait qui se rapproche de ces photos sans toutefois être une copie exacte. Or, dans un avenir proche, il est estimé qu'ils seront en mesure d'imiter entièrement les corps, têtes et même les voix d'une façon quasi authentique. Bien que des capacités décuplées alimentent nombre de craintes pour le futur, les *deepfakes* sont d'ores et déjà la cause de nombreux préjudices sur Internet, notamment en ce qui a trait à la pornographie non consensuelle.

Naissance d'une industrie pornographique

Les vidéos humoristiques, tels que le fameux *deepfake* du président Obama réalisé par Jordan Peel, ne représentent qu'un faible pourcentage des contenus du genre produits actuellement. En effet, selon la firme Sensity, en 2019, 96 % de tous les *deepfakes* partagés publiquement étaient de nature pornographique. Il existe sur Internet une importante communauté de comptes dédiés à la création et au partage de *deepfakes* à contenu pornographique, qui interagit sur des forums et des chats cryptés. Il est d'ailleurs estimé que ces communautés regroupent au total plus de 100 000 membres. N'importe qui peut désormais payer pour faire développer des *deepfakes* pornographiques personnalisés. En outre, ces forums sont aussi le théâtre de concours pour déterminer qui parvient à créer la meilleure vidéo pornographique.

Une des applications qui facilite l'accès aux technologies sous-jacentes aux *deepfakes* est DeepNude. Lancé en 2019, ce service permet aux utilisateurs de « dénuder » des photos de femmes habillées, les algorithmes d'apprentissage ayant été réglés pour

retirer synthétiquement les vêtements des images de femmes et générer des parties nues de leur corps. Ces algorithmes ne peuvent pas effectuer des transformations similaires sur des images d'hommes puisqu'ils ont été spécifiquement entraînés sur des images de femmes. Selon DeepNude, en juin 2019, l'application aurait reçu 545 162 visites et comptait 95 464 de profils actifs, la majeure partie de cette activité s'étant probablement produite au cours d'une période de 24 heures suivant son lancement.

Bien que depuis, le site ait été mis hors ligne, le logiciel continue d'être reconditionné et distribué de manière indépendante en ligne. De fait, deux nouveaux portails de services ont ouvert, avec des tarifs allant de 1 $ à 20 $ par photo. La demande est énorme et contribue à ce que le logiciel continue de se répandre, devenant ainsi un outil populaire pour créer de la pornographie non consensuelle de type *deepfake*.

Un nouvel outil de sextorsion : les *ransomfakes*

Alors que ces technologies deviennent de plus en plus accessibles, les actes de chantage et les sextorsions utilisant des *deepfakes* à caractère pornographique sont en hausse. Baptisées *ramsomfakes*, ces attaques s'appuient sur l'utilisation d'un logiciel malveillant qui génère automatiquement une fausse vidéo montrant la victime en train d'effectuer une action incriminante ou intime, suivie d'une menace de la diffuser si une rançon n'est pas payée. À l'instar de nombreux autres cybercriminels, les auteurs de ces attaques exigent fréquemment d'être payés en cryptomonnaies, afin de diminuer leur traçabilité financière.

Plus inquiétant encore, il existe désormais des bots programmés pour explorer constamment le Web à la recherche d'images et de vidéos de femmes, à partir de leurs propres comptes de réseaux sociaux, pour créer des *deepfakes* pornographiques et éventuellement mener à des attaques de type *ramsomfake*. De manière générale, trois préjudices pour les femmes ont été mentionnés dans la couverture médiatique de ce phénomène : la détresse émotionnelle et psychologique, la perte d'autonomie sur son corps et sa réputation, et le lien entre les *deepfakes* et d'autres crimes éventuels[3]. En effet, les cibles des *deepfakes* deviennent des victimes d'abus et de crimes identifiables tels que le harcèlement, la diffamation, le chantage et l'extorsion.

De la diffamation aux campagnes de chantage politique

En plus de ces activités à but lucratif, l'utilisation de *deepfakes* à des fins de discrédition de personnalités en position de pouvoir est de plus en plus commune. En 2018, après avoir été invitée par de grands médias à commenter les circonstances entourant le viol d'une fillette cachemirienne de huit ans, la journaliste indienne Rana Ayyub fut victime d'une campagne massive de dénigrement en ligne. Un des outils de cette campagne a été la création d'une vidéo de *deepfake* pornographique représentant le visage de la journaliste superposé au corps d'une personne non identifiée en train de performer un acte sexuel. Selon Ayyub, la vidéo a été partagé plus de 40 000 fois via les médias sociaux par des agent.e.s subalternes du Bharatiya Janata Party[4], ainsi que des trolls

[3] Gosse, C. et Burkell, J. (2020). Politics and Porn: How News Media Characterizes Problems Presented by Deepfakes. *Critical Studies in Media Communication*, *37*(5), 497-511.

[4] Le Baharatiya Janata Party est un des deux principaux partis politiques indiens, le BJP est un parti de droite nationaliste hindou.

d'extrême droite ou d'autres internautes. La mise en ligne du *deepfake* s'est accompagnée de *doxing*[5] : les harceleurs d'Ayyub ont publié son numéro de téléphone, menant à la réception de nombreux messages lui demandant combien elle chargeait pour des relations sexuelles[6].

Le cas n'est pas unique en son genre : en 2016 aux Philippines, le conseiller juridique du président Rodrigo Duterte a utilisé un vidéo sexuel truqué de la sénatrice Leila De Lima pour justifier son emprisonnement, visiblement en représailles à ses critiques du régime[7]. En Indonésie, à l'approche des élections indonésiennes de 2019, Grace Natalie, cheffe du Parti de la solidarité indonésienne (PSI), a été la cible d'une attaque similaire : un compte Twitter anonyme nommé Hulk a accusé la politicienne d'entretenir une relation extraconjugale avec Pak Ahok, l'ancien gouverneur de Jakarta. L'accusateur menaçait de rendre publique une vidéo pornographique des deux individus. Bien que Grace Natalie a défié son maître chanteur de publier le prétendu film, plusieurs observateurs ont noté qu'un *deepfake* aurait potentiellement suffit à discréditer la politicienne[8].

Ces deux cas sont des exemples frappants de la sexualité féminine utilisée comme une arme par leurs adversaires politiques, et de l'utilisation de *deepfakes* pornographiques comme moyens de pression politique. Or, ni l'une ni l'autre des femmes visées n'ont vu leurs accusateurs tenus responsables de la diffusion de fausses informations à caractère sexuel destinées à les salir. La technologie *deepfake* ne cesse de s'améliorer, d'où l'importance d'en étudier les possibles conséquences. Les campagnes de désinformation disposent à l'avenir d'une arme puissante pour exploiter la sexualité des femmes dans le but d'affaiblir des adversaires politiques ou même, dans certains pays, justifier leur incarcération.

Plusieurs enjeux encore invisibles dans les médias

La littérature actuelle sur l'enjeu des *deepfakes* identifie deux grandes lacunes dans le traitement médiatique du problème. Premièrement, bien que porteuses d'énormes conséquences, les sextorsions utilisant des *deepfakes* à contenu pornographique sont considérées comme étant moins préoccupantes dans l'œil du public que les *deepfakes* déployés à des fins politiques, pour de la propagande notamment. La couverture médiatique qui traite des *deepfakes* pornographiques élude grandement les préjudices personnels et collectifs associés aux *deepfakes* sexuels, rendant donc ces conséquences et les victimes invisibles aux yeux du public. Samantha Bates souligne par ailleurs que lorsque les cibles des *deepfakes* pornographiques sont discutées, l'accent est mis sur les femmes dont le visage est utilisé, et non sur les personnes dont le corps est

[5] « Publication intentionnelle sur internet d'informations personnelles sur un individu par un tiers, souvent dans le but d'humilier, menacer, intimider ou punir l'individu en question » (Douglas, 2016).

[6] Paris, B. et Donovan, J. (2019). Deepfakes and cheap fakes: the Manipulation of Audio and Visual Evidence, *Data & Society*, https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf

[7] De Lima on Sex Video: It Is Not Me (6 octobre 2016). *Philstar Global.* https://www.philstar.com/headlines/2016/10/06/1630927/de-lima-sex-video-it-not-me

[8] Davis, M. J. et Fors, P. (2020). Towards a Typology of Intentionally Inaccurate Representations of Reality in Media Content. *Springer International Publishing*, 291-304.

instrumentalisé. De plus, la couverture médiatique se concentre sur les femmes cisgenres et n'a pas encore étendu sa discussion aux personnes trans ou non binaires, elles aussi victimes de tels crimes[9].

Deuxièmement, Sophie Maddocks souligne que les discussions sur l'identité des auteur.e.s de *deepfakes* pornographiques, et sur les facteurs culturels favorisant cette transgression, sont totalement absentes de la couverture médiatique. Alors qu'un grand nombre de femmes ont vu leurs images trafiquées sur le plan sexuel, l'utilisation de *deepfakes* à de telles fins s'inscrit dans un modèle socioculturel plus large de comportements misogynes. Ce lien entre les *deepfakes* pornographiques et la misogynie d'ordre systémique est majoritairement négligé, et même absent des discours véhiculés dans la presse[10].

De plus en plus fréquent, ce genre de cas met en lumière de graves enjeux pour le respect des droits humains et le droit à la vie privée, au Canada et ailleurs. Les *deepfakes* à caractère sexuel représentent un enjeu important pour l'engagement du Canada en faveur d'une politique étrangère féministe : tout indique en effet que les efforts consacrés à l'élimination de la violence et des abus faits aux femmes se heurteront, dans les années à venir, de plus en plus fréquemment aux enjeux entourant les *deepfakes*. Il importe donc de saisir dès maintenant les tenants et aboutissants de ce phénomène.

2. SEXTORSION : PORTRAIT DU PHÉNOMÈNE

2.1. Prévalence des actes de sextorsion

Le phénomène de la sextorsion se trouve à l'intersection des violences sexuelle, psychologique, économique et informatique. Ainsi, pour capter l'éventail des manifestations de la sextorsion, nous en avons favorisé une large définition selon une approche privilégiée par les chercheurs et chercheuses dans le domaine des violences sexuelles en ligne (Carlton, 2019; Fortin et Desfachelles, 2019; Henry et Flynn, 2019; McGlynn *et al*., 2017). Encore aujourd'hui, l'utilisation d'images intimes pour manipuler, humilier et contrôler un individu n'est pas communément reconnue en tant que manifestation de violence à caractère sexuel, surtout lorsqu'il est question de victimes adultes (McGlynn *et al*., 2017). On désigne le phénomène plutôt comme une atteinte à la vie privée ou comme une forme d'intimidation. Pourtant, la violence à caractère sexuel dans la sphère numérique est abordée et punie lorsqu'il est question de victimes mineures (p. ex. pornographie juvénile, leurre informatique). Il est impératif que la sextorsion visant des adultes soit considérée en tant que crime sexuel au même titre que la violence sexuelle avec contacts physiques. Tel que l'indiquent McGlynn et ses collègues (2017) : « la nature sexuelle de l'acte; l'atteinte à la dignité, à l'autonomie et à l'expression sexuelle; la minimisation des abus dans le discours public; les dynamiques de genre; ne sont

[9] Bates, S. (2017). Revenge Porn and Mental Health. *Feminist Criminology*, *12*(1), 22-42.

[10] Maddocks, S. (2020). 'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities Between Pornographic and 'Political' Deep Fakes. *Porn Studies*, *7*(4), 415-423.

que quelques manifestations qui témoignent du caractère commun entre les VCSBI et les violences sexuelles avec contact » (traduction libre, pp. 28-29).

Il est particulièrement difficile d'obtenir un portrait juste de la prévalence des actes de sextorsion perpétrés dans la population. Premièrement parce que la reconnaissance sociale et juridique de la sextorsion en tant que crime à part entière est relativement nouvelle (Feigenblatt, 2020). Par conséquent, de nombreux actes de sextorsion ont été répertoriés dans les textes juridiques et dans les rapports statistiques sous une autre appellation. Selon Feigenblatt (2020), le terme « sextorsion » est utilisé de façon interchangeable avec, par exemple, le « harcèlement sexuel ». Deuxièmement, les actes de sextorsion seraient fortement sous-déclarés, faute de procédures juridiques adéquates, voire de soutien suffisant pour les victimes (Feigenblatt, 2020). En effet, il n'existe toujours aucun article de loi traitant spécifiquement de la sextorsion au Canada, cette dernière étant fréquemment classifiée sous d'autres crimes sexuels, tels que la production de pornographie juvénile, le partage non consensuel d'images intimes, le leurre informatique ou l'extorsion. Enfin, peu d'attention est portée à la victimisation sexuelle des adultes dans la sphère numérique : la sextorsion est davantage étudiée auprès des enfants, des adolescent.e.s ou des jeunes adultes. Lorsqu'elles portent sur une population adulte, la majorité des études sont menées auprès d'étudiant.e.s universitaires, sur des groupes d'âge très restreints et auprès d'échantillons de populations relativement homogènes (peu de personnes de la diversité culturelle, sexuelle et de genre), ce qui rend les conclusions de recherche difficilement généralisables (Drouin et Tobin, 2014; Fortin et Desfachelles, 2019; Henry et Powell, 2018; McGlynn *et al*., 2017). De plus, en ce qui concerne la méthodologie, certain.e.s auteur.e.s mobilisent une lecture dichotomique pour documenter la victimisation et la perpétration de la sextorsion, c'est-à-dire que les études ne font qu'explorer la présence ou l'absence du vécu de sextorsion (Patchin et Hinduja, 2020), ce qui limite la compréhension du phénomène. Tel que mentionné par Patchin et Hinduja (2020), il serait pertinent de documenter la prévalence d'actes de sextorsion en fonction de leurs caractéristiques, notamment la nature de la relation entre la victime et le sextorqueur ou la sextorqueuse, la récurrence des menaces, le moment auquel les actes de sextorsion se sont produits ou encore le type de contenu ayant été partagé ou menacé de partager.

Bien qu'il n'existe pas de données officielles en ce qui concerne le nombre d'actes de sextorsion perpétrés dans la population, les statistiques présentées au sein d'études empiriques, de rapports gouvernementaux et d'articles de journaux permettent de constater l'ampleur du problème et l'importance de s'y intéresser davantage. Selon une étude récente menée auprès de 5568 jeunes d'entre 12 et 17 ans aux États-Unis, 3 % ont admis avoir menacé de partager des images ou des vidéos sexuellement explicites d'une autre personne sans son consentement, et 5% ont déclaré avoir été victimes de sextorsion (Patchin et Hinduja, 2020). De façon similaire, selon une recherche effectuée auprès de 4053 Australien.ne.s, plus de 11 % des répondant.e.s rapportaient avoir commis une violence à caractère sexuel basée sur l'image au cours de leur vie, dont les deux plus courantes formes sont la distribution d'une image intime (6,4 %) et la menace de distribuer une image intime (4,9 %) (Powell *et al*., 2019). Selon Lenhart et ses collègues (2016), 3 % des internautes en provenance des États-Unis ont reçu des menaces de distribution non consensuelle d'images intimes, et 2 % l'ont réellement vécu. Dans une autre étude menée auprès de 4274 personnes âgées entre 16 et 49 ans en Australie, plus de 20 % ont rapporté avoir été photographié.e.s en contexte intime sans leur consentement. Les images sexuellement explicites furent distribuées dans 45 % des cas, et 9 % des répondant.e.s ont

déclaré avoir reçu des menaces visant le partage potentiel de leurs images sexuellement explicites (Henry *et al*., 2017).

De plus en plus d'annonces gouvernementales concernant la prévalence alarmante de la sextorsion sont publiées au cours des dernières années. À titre d'exemple, en février 2022, la Gendarmerie royale du Canada a publié un communiqué de presse concernant une hausse de plus de 62 % des cas de sextorsion auprès des jeunes à Terre-Neuve. Selon Statistique Canada, de 2012 à 2018, les évènements d'extorsion rapportés à la police auraient augmenté de 170 % (1730 vs 4664 cas). Cette augmentation serait principalement due aux cas de sextorsion en ligne. En ce sens, la responsable de l'Unité d'exploitation sexuelle des mineurs (ESM) du Service de police de la ville de Québec (SPVQ), Marie-Manon Savard, estime que nous faisons face à une réelle explosion des cas de sextorsion. Selon elle, un nouveau cas de sextorsion impliquant des personnes mineures est rapporté à tous les jours et des arrestations pour leurre ou extorsion sont faites à chaque semaine. À son avis, ces chiffres seraient beaucoup plus élevés si l'unité possédait les ressources et les effectifs supplémentaires (Cloutier, 2021). L'organisme Cyberaide rapporte une augmentation de 88 % des cas de cybersextorsion envers les enfants depuis le début de la pandémie, soit plus de 40 évènements rapportés par mois (Somos, 2021). Enfin, en 2021, la Sûreté du Québec rapportait que les cas de jeunes garçons de 12 à 17 ans victimes de sextorsion avaient triplé (Rivard, 2021). De plus, Cyberaide rapportait à Global News une augmentation de 88 % des cas de sextorsion depuis le début de la pandémie (Slugosky, 2021).

En ce qui concerne les actes de sextorsion qui n'ont pas de composantes technologiques, c'est-à-dire qui prennent place dans le monde physique, encore très peu d'études empiriques nous éclairent quant à leur prévalence. Toutefois, en 2019, une étude du *TI Global Corruption Barometer* révèle qu'en Amérique latine, au Moyen-Orient et en Afrique du Nord, une personne sur cinq aurait été victime ou connaîtrait une personne ayant été victime de sextorsion alors qu'elle tentait d'accéder à des services gouvernementaux. Cette statistique rend compte de l'ampleur de l'enjeu de la sextorsion dans l'accès à des services publics (Ferguson, 2022). Qui plus est, les femmes et les personnes de la diversité sexuelle et de genre seraient touchées de manière disproportionnée par la sextorsion de type corruption. Ces statistiques révèlent le besoin imminent de développer des connaissances sur ce phénomène très peu étudié, qui va à l'encontre des droits de la personne, et qui touche directement à des enjeux se rapportant à l'égalité des genres (Feigenblatt, 2020).

2.2. Portrait des victimes

La sextorsion touche l'ensemble de la population mondiale, des classes et des groupes d'âge (Feigenblatt, 2020). S'il est généralement admis que les victimes de sextorsion sont majoritairement des femmes (Henry et Powell, 2018; Wolak et Finkelhor, 2016), les hommes et les personnes de la diversité de genre sont également les cibles de sextorsion (Eaton *et al.*, 2022; Lenhart, Y'barra et Feeney-Price, 2016; Powell et Henry, 2016). Au sein de l'étude de Wolak et Finkelhor (2016) menée auprès de 1631 victimes de sextorsion âgées entre 18 et 24 ans, 89 % des victimes étaient des femmes contre 11 % d'hommes. Cependant, la prévalence de la sextorsion en fonction du genre ne fait pas l'unanimité : d'autres études empiriques ont

plutôt documenté que les hommes sont plus fréquemment victimes de sextorsion (Patchin et Hinduja, 2020). Cet écart pourrait être expliqué en fonction du type de sextorsion; les hommes semblent en être davantage la cible lorsque les demandes sont de nature monétaire, alors que les femmes sont plus souvent visées lorsque les requêtes sont d'ordre sexuel (O'Malley et Holt, 2020).

Qui plus est, plusieurs auteur.e.s rapportent que les personnes noires et/ou autochtones, LGBTQ+, en situation de handicap, et les jeunes adultes seraient surreprésentées chez les victimes de violence à caractère sexuel en ligne (Borrajo *et al*., 2015; Eaton *et al*., 2022; Henry *et al*., 2017; Lenhart *et al.*, 2016; Patchin et Hinduja, 2020). Ainsi, à l'instar des violences à caractère sexuel, psychologiques, économiques et informatiques, la sextorsion semble viser de façon disproportionnée les populations marginalisées, entre autres sur la base de l'identité de genre, de l'orientation sexuelle, de la couleur de peau et/ou de l'origine ethnoculturelle. L'intersection entre ces divers éléments identitaires produisant des réalités uniques, il est impératif de mobiliser une approche intersectionnelle afin d'analyser et de lutter contre ce crime sexuel, car cette approche permet le développement d'interventions adaptées aux besoins et aux réalités des personnes victimes.

2.3. Profils des sextorqueurs et sextorqueuses

Considérant que les technologies permettent d'aller bien au-delà des cercles sociaux de proximité, le sextorqueur ou la sextorqueuse peut fort bien être inconnu.e de la victime et travailler de partout autour du globe. Dans ce cas, les actes de sextorsion sont bien souvent commis par des *scammers* qui ont recours à des identités frauduleuses afin d'attirer des victimes et de créer un lien de confiance (*catfishing)*. Pour y arriver, plusieurs pratiquent le *capping* en multipliant les victimes ou en agissant au sein d'un groupe de sextorqueurs et sextorqueuses professionnel.le.s qui ont généralement comme motivation le gain financier (Agence France Presse, 2014).

Après avoir analysé 152 cas de sextorsion en ligne rapportés dans les médias, O'Malley et Holt (2020) ont relevé quatre catégories de cybersextortion pouvant être classées en fonction du type de sextorsion perpétué. O'Malley et Holt recensent ainsi la sextorsion 1) auprès de personnes mineures, 2) axée sur la cybercriminalité, 3) intimement violente et 4) criminelle transnationale. Ces quatre catégories de cybersextortion diffèrent en ce qui a trait à leurs méthodes, leurs motivations, leurs demandes et leurs victimes. Alors que la première catégorie cible spécifiquement des victimes de moins de 18 ans, les autres n'ont pas de préférence en termes d'âge (O'Malley et Holt, 2020). Les individus perpétrant de la sextorsion intimement violente ciblent plus souvent des femmes de leur entourage, alors que ceux qui commettent de la sextorsion à l'endroit de personnes mineures et la cybercriminalité vont plus souvent cibler des personnes inconnues de différentes identités de genre. Pour ce qui est de la sextorsion transnationale, les hommes seraient majoritairement visés par ce type de crime (O'Malley et Holt, 2020).

Bien que l'ensemble des cybersextorqueurs et cybersextorqueuses utilisent la manipulation afin d'extorquer leurs victimes, leurs méthodes diffèrent (O'Malley et Holt, 2020). Ceux et celles perpétrant de la cybersextorsion auprès de personnes mineures (cat. 2) le

font en bâtissant une relation de confiance avec leurs victimes avant de procéder au chantage et d'exiger des faveurs sexuelles. En revanche, les individus perpétrant de la sextorsion axée sur la cybercriminalité (cat. 3) et de la sextorsion transnationale (cat. 4) utilisent des logiciels malicieux (maliciels) afin d'obtenir du contenu sexuellement explicite, et ont tendance à effectuer leurs demandes beaucoup plus rapidement (O'Malley et Holt, 2020). Quant aux rançons, alors que les deux premières catégories cherchent principalement à obtenir des faveurs sexuelles ou du contenu sexuellement explicite, celle de la sextorsion intimement violente (cat. 3) vise à contrôler les comportements des victimes et à acquérir des gains majoritairement non sexuels tels que la continuité d'une relation amoureuse avec la victime. Pour ce qui est des individus perpétrant de la sextorsion criminelle transnationale, leurs motivations sont strictement financières : ils veulent de l'argent en échange d'images ou de vidéos sexuellement explicites obtenues sans le consentement des victimes (O'Malley et Holt, 2020). Malgré le fait que ces quatre catégories de sextorsion comportent des caractéristiques différentes, elles ont toutes un point en commun, c'est-à-dire qu'elles « impliquent un sentiment de pouvoir et de contrôle sur la victime qui est exercé et maintenu [par exemple], par la menace de distribuer des images par des moyens technologiques » (traduction libre de O'Malley et Holt, 2020, p. 17).

Plusieurs évènements rapportés dans la littérature scientifique et dans les médias révèlent enfin que les sextorqueurs et sextorqueuses sont souvent dans l'entourage des personnes victimes. Dans ce cas, les actes de sextorsion s'inscrivent dans un contexte plus large de violence interpersonnelle ou de violence domestique et se déroulent généralement à la maison, au travail ou à l'école. En effet, de plus en plus de cas de sextorsion ont lieu au sein de relations intimes, surtout chez les jeunes (Cloutier, 2021). Selon Joanny St-Pierre, procureure et coordonnatrice du comité de concertation en matière de lutte contre l'exploitation sexuelle des enfants sur Internet, il est impératif de lutter contre la représentation populaire voulant que les sextorqueurs sont des hommes adultes, inconnus de la victime, et opérant uniquement dans la sphère numérique. Ces représentations unidimensionnelles soutiennent par ailleurs une vision étriquée de la sextorsion, qui se limite généralement aux violences sexuelles basées sur l'image ou au partage non consensuel d'images intimes.

2.4. Contextes dans lesquels la sextorsion a lieu

Après avoir effectué une étude auprès de 1631 victimes de sextorsion âgées de 18 à 24 ans, Wolak et Finkeldor (2016) ont documenté deux contextes distincts dans lesquels se déroulent les actes de sextorsion. D'une part, dans la majorité des cas (60 %), les personnes victimes avaient déjà rencontré leur sextorqueur ou sextorqueuse, qui s'avérait être un.e ancien.ne ou un.e nouvel.le partenaire, un.e ami.e ou encore un.e collègue de travail. D'autre part, les actes de sextorsion étaient commis par des personnes rencontrées par l'entremise du numérique; dans ces cas spécifiques, les victimes n'avaient jamais eu de contact physique avec leur sextorqueur ou sextorqueuse. Selon Wolak et Finkeldor (2016), ces deux contextes comportent des caractéristiques différentes, notamment en ce qui a trait à la nature des menaces et la dynamique de la relation entre la victime et le sextorqueur ou la sextorqueuse.

Dans un premier temps, Wolak et Finkelhor (2016) ont documenté une différence quant à l'identité de genre des victimes en fonction du contexte. Alors que les femmes représentaient 87 % des victimes dans les relations interpersonnelles (relations incluant des contacts physiques entre les partenaires), elles représentaient plutôt 77 % des victimes dans les relations exclusivement en ligne. Pour ce qui est des hommes, l'effet inverse est observé : ces derniers représentaient 11 % des victimes dans les relations en face à face, contre 20 % dans les relations exclusivement en ligne. De plus, davantage de victimes de sextorsion dans les relations en face à face ont envoyé des images de manière consensuelle, soit 75 % contre 65 % dans les relations en ligne, et ce, principalement puisqu'elles se trouvaient dans des relations romantiques ou sexuelles avec leur agresseur ou agresseuse. Cependant, bien que 40 % des répondant.e.s aient soulevé avoir envoyé du contenu à caractère sexuel de manière consensuelle, plus de 56 % se sont senti.e.s forcé.e.s de le faire. Dans les deux contextes, pour plus de 45 % des cas de sextorsion, le contenu sexuellement explicite a été obtenu de manière non consensuelle, notamment sans que la victime en ait connaissance. Une différence est également observée en ce qui a trait au temps écoulé entre la rencontre des individus impliqués et l'envoi de matériel sexuellement explicite. Alors que 27 % des victimes de sextorsion dans les relations en ligne ont envoyé pour la première fois du contenu à caractère sexuel après 24 heures, seulement 2 % d'entre elles l'ont fait dans le cadre de relations en face à face. D'autre part, alors que 59 % des victimes de sextorsion dans les relations en face à face ont envoyé du contenu sexuellement explicite pour la première fois à leur sextorqueur ou sextorqueuse après trois mois, ce pourcentage représente seulement 10 % des victimes de sextorsion dans les relations en ligne.

Dans un deuxième temps, des différences ont également été observées en ce qui a trait à la nature des menaces dans les deux contextes. Alors que la majorité des sextorqueurs et sextorqueuses dans les relations en face à face souhaitaient maintenir ou restaurer la relation avec la victime, ceux et celles dans des relations en ligne voulaient plutôt obtenir du contenu à caractère sexuel, des faveurs sexuelles ou encore un montant d'argent (Wolak et Finkeldor, 2016). Plusieurs répondant.e.s ont reçu des menaces de préjudices physiques à leur égard ou à l'endroit de leurs familles, ami.e.s ou animaux domestiques. Certain.e.s répondant.e.s de la diversité sexuelle et de genre ont également rapporté avoir reçu des menaces concernant l'exposition de leur identité à leur famille ou ami.e.s. Cette dynamique peut être particulièrement dangereuse dans certains milieux ou pays hostiles envers les personnes LGBTQ+. En ce qui concerne le moment auquel la première menace survient, la durée et la fréquence des menaces, ces dernières étaient beaucoup plus rapides, fréquentes et courtes au sein des relations en ligne (Wolak et Finkeldor, 2016).

3. SEXTORSION ET NOUVELLES TECHNOLOGIES

3.1. Internet et les violences à caractère sexuel

Afin de comprendre, d'analyser et de contrer la sextorsion, il importe d'aborder l'avènement des nouvelles technologies et leurs conséquences potentielles sur la vie des individus. Une recherche menée par Navarro et Jasinski (2013) montre qu'un nombre élevé d'heures de navigation sur Internet serait corrélé positivement avec un plus haut risque de victimisation en ligne. Ainsi, ce serait la fréquence des interactions interpersonnelles en ligne

qui influencerait le risque d'être victime ou auteur.e de cyberviolence (Holt et Bossler, 2007; Marcum, 2008; Mesch, 2009). Cependant, ce facteur de risque manque de précision considérant que la vaste majorité de la population mondiale entretient des relations interpersonnelles en ligne sans être forcément victime ou auteur.e de cybercrimes. D'autres auteur.e.s, pour leur part, identifient certains comportements sociaux qui augmentent les chances de cybervictimisation en facilitant la proximité avec les potentielles personnes agresseuses, notamment le fait d'accepter des demandes d'amitié ou de discuter avec des personnes inconnues sur les réseaux sociaux (Reyns *et al.*, 2011; Vakhitova *et al*., 2019). Toutefois, davantage de recherches seraient nécessaires afin d'établir les facteurs de risque et de protection liés aux violences à caractère sexuel en ligne.

Pour plusieurs, les TIC constituent un médium intéressant afin d'entamer et d'alimenter des relations intimes et sexuelles (Fortin et Desfachelles, 2019). En effet, la démocratisation d'Internet aurait engendré une véritable révolution sexuelle (Garlick, 2011). Selon plusieurs auteur.e.s, Internet élargit les possibilités en matière de sexualité en permettant, entre autres, aux individus se trouvant aux quatre coins du monde de créer et de maintenir des liens intimes malgré la distance physique (Buhi *et al*., 2014; Koch et Miles, 2021), et offre également aux individus la possibilité de créer et de distribuer leur propre pornographie, une pratique s'avérant, pour certain.e.s, une façon d'explorer et d'exprimer sa sexualité (Buhi *et al*., 2014). À l'ère pandémique, les diverses technologies et l'utilisation de la webcam ont permis à certaines personnes de maintenir la satisfaction sexuelle et le désir malgré l'absence de contacts physiques avec des partenaires (Eleuteri et Terzitta, 2021). En bref, depuis les années 2010, Internet est de plus en plus utilisé dans un but d'épanouissement sexuel puisqu'il permet entre autres d'entretenir des relations intimes, d'offrir de nouvelles opportunités de rencontres et de contribuer au plaisir solitaire (Garlick, 2011). Il offre également aux individus un espace plus confortable pour échanger lorsqu'il est question de discuter d'enjeux de nature sexuelle, considérant qu'un certain anonymat peut être conservé (Buhi *et al.*, 2014; Koch et Miles, 2021). Toutefois, tel que mentionné précédemment, les nouvelles technologies font également émerger de nombreux défis nécessitant une plus grande attention, notamment en ce qui a trait à la reproduction des dynamiques de violences à caractère sexuel dans la sphère numérique (Aikens, 2016) ou à l'effet de chambre à écho[11] pour des pensées et des attitudes radicales (Hassan, 2018). En effet, selon Holt et Ligget (2020), l'ère numérique permet aux groupes défendant des intérêts et des pensées radicales de transmettre leur idéologie à grande échelle et auprès d'un grand nombre d'individus. Ainsi, bien que l'ère numérique facilite l'exploration et l'expression de sa sexualité (Buhi *et al*., 2014), elle comporte également des risques considérables en termes de reproduction de dynamiques de pouvoir, de systèmes de classes, de race et de violence sexuelle, d'où l'importance d'adopter une approche nuancée afin d'aborder les questions touchant à la sexualité et aux technologies (Koch et Miles, 2021).

Plusieurs théories peuvent être mobilisées afin de comprendre la sextorsion à l'aune des nouvelles technologies. L'une d'entre elles est l'approche des activités routinières. Introduite en 1979 par Felson et Cohen, elle est utilisée pour déterminer les facteurs

[11] L'effet de chambre à écho est un biais de confirmation au sujet de l'accès à l'information. Celui-ci se concrétise dans un contexte où les individus sont constamment renvoyés uniquement à du contenu qui confirme leurs croyances. Ce phénomène est particulièrement présent dans les médias sociaux participatifs, où la sélection d'information et les algorithmes personnels limitent l'exposition à des points de vue divergents.

situationnels qui mènent à l'occurrence de certains délits. Cette approche permet d'accroître la compréhension d'un phénomène criminel, du contexte dans lequel il a lieu ainsi que des parties impliquées. Considérant qu'elle permet également de mettre en place des stratégies de prévention et des programmes d'éducation adaptés en raison des composantes qu'elle documente, cette approche est particulièrement mobilisée pour l'étude de divers phénomènes criminels. L'approche des activités routinières postule qu'un crime est possible lorsqu'il y a convergence dans le temps et l'espace de trois facteurs : un individu motivé, une cible vulnérable et l'absence d'un.e gardien.ne capable de prévenir le crime (p. ex : police, système d'alarme). Cette approche met en lumière le fait que des actes délictuels prennent place au sein de la vie quotidienne et que leur mise en place est influencée par les comportements et l'environnement propres aux personnes impliquées. Ainsi, ce sont les changements socio structurels dans les activités quotidiennes qui transforment la « chimie du crime ». La chimie du crime réfère ici à la convergence dans le temps et l'espace de la cible vulnérable et d'un individu motivé en l'absence de gardien.ne.s capables (Felson, 1998). L'approche des activités routinières nous permet d'identifier des stratégies de prévention situationnelle qui permettent de prévenir les délits en intervenant en amont sur l'environnement et les individus. La prévention situationnelle est une mesure qui augmente le coût et diminue les bénéfices du passage à l'acte criminel.

Une précision s'impose lorsqu'on applique cette approche à la cybercriminalité puisqu'à la différence des crimes avec contact, les entités sur le Web, c'est-à-dire les personnes, le contenu et les plateformes ne peuvent être localisées dans un espace-temps fixe et défini. L'absence de frontière spatiale et temporelle en ligne nous invite à redéfinir les concepts de temps et d'espace. En effet, Internet offre un accès continu à une infinité de lieux interactifs et interreliés; on peut désormais porter atteinte instantanément à une personne sans contact physique. Selon certain.e.s auteur.e.s, cette convergence du temps et de l'espace est une constante, ce qui multiplie les risques de victimisation (Reyns *et al*., 2011). En effet, l'étendue d'Internet, mais également la permanence du contenu en ligne, permettent de porter atteinte à l'intégrité d'un individu qui n'est pas activement présent dans l'environnement Web au moment où le geste est commis. En raison de l'effondrement du temps et de l'espace sur le Web, la violence peut désormais suivre l'individu en toutes circonstances. De cette manière, la technologie numérique permet d'étendre des situations de violence domestique en facilitant des comportements de contrôle coercitif par le truchement de la technologie, comme le harcèlement et les menaces répétées, l'espionnage clandestin par la géolocalisation ou par l'enregistrement audio ou visuel, l'accès non autorisé aux comptes personnels et le contrôle de l'accès à Internet (Dragiewicz *et al*., 2018a; 2018b).

Selon l'approche des activités routinières, la présence d'une surveillance formelle (p. ex. rempart juridique) ou informelle (p. ex. gardien de sécurité) diminue les chances de commettre un acte criminel. Pour ce qui est de la sextorsion, outre l'article 346(1) du Code criminel canadien (1985), il n'existe que peu de remparts formels contre ce type de crime. Internet est un lieu peu régulé et les législations peinent à s'adapter à l'évolution rapide des technologies et au besoin de collaboration internationale contre la cybercriminalité (GRC, 2015). En raison de l'inadaptation des lois visant à punir des actes criminels en ligne posés par une personne d'un autre pays et la sophistication des techniques d'anonymisation, ces crimes restent difficiles à appréhender. À ces défis s'ajoutent la multiplicité des victimes parfois

dispersées à travers le monde, les difficultés d'identification des auteur.e.s de cybercrime et la réticence des victimes à témoigner (Saint-Louboue, 2020).

Face à l'ubiquité des technologies de l'information, un autre enjeu de taille se pose : leur développement est si rapide que les techniques utilisées pour commettre des actes violents se développent plus rapidement qu'il n'est possible de les comprendre. Bien que certaines recherches montrent que l'utilisation d'un antivirus est corrélée négativement avec les crimes qui ciblent la technologie, l'antivirus serait peu protecteur contre certains types de cyberviolence interpersonnelle tels que le cyberharcèlement (Holt et Bossler, 2007; Reyns *et al*., 2016). Certaines recherches montrent que les individus ayant de bonnes connaissances informatiques et une conscience des risques courus en ligne seraient moins à même d'être victimes de cyberviolence puisque leurs connaissances agiraient comme une forme d'autoprotection. Ces résultats ont d'ailleurs été démontrés au sein de l'étude de Leukfeldt et Yar (2016) qui aborde la cybervictimisation.

En conclusion, bien que l'architecture du Web puisse contribuer à faciliter certains délits, Dodge et Spencer (2018) mettent en garde contre la peur des nouvelles technologies qui peut entraîner une panique morale et une pathologisation des comportements sexuels en ligne. Ces nouvelles technologies servent parfois de boucs émissaires pour des problèmes sociaux plus importants tels que la culture du viol, sur lesquels il importe de se pencher pour prévenir les violences à caractère sexuel en ligne.

4. IMPACTS DE LA SEXTORSION CHEZ LES VICTIMES

La sextorsion engendre de nombreuses conséquences chez les victimes, et ce, tant au niveau psychologique, physique, sexuel, économique que social (Feigenblatt, 2020). Après avoir examiné 78 cas judiciaires de sextorsion, Wittes et ses collègues (2016) rapportent que les victimes disent ressentir de l'impuissance et de la vulnérabilité, ainsi qu'un état continuel de peur et d'anxiété face à la possibilité que leur détracteur ou détractrice les exposent ou les soumettent à de nouvelles requêtes (Wittes *et al*., 2016). Les victimes sont également particulièrement isolées; elles se sentent sous l'emprise de leur sextorqueur ou sextorqueuse et disent avoir l'impression de ne pouvoir se confier à personne en raison d'un sentiment de honte ou de culpabilité, ou par crainte des conséquences sociales, légales ou professionnelles (Wittes *et al*., 2016). Outre l'anxiété, les victimes de sextorsion sont également à risque de vivre des épisodes dépressifs (Hong, *et al.* 2020), et certaines victimes sentent l'obligation de déménager suite aux évènements de sextorsion (Wolak et Finkelhor, 2016).

Au niveau social, Wittes et ses collègues (2016) rapportent également que les jeunes victimes sont davantage exposées à la double victimisation : en plus d'être victimes de sextorsion, la responsabilité de leur agression leur serait attribuée sous prétexte qu'elles aient cédé aux menaces de leurs détracteurs ou détratrices, ou qu'elles aient partagé des images intimes (Wittes *et al*., 2016). Certaines victimes de sextorsion, plus spécifiquement les femmes, peuvent également être aux prises avec un sentiment de honte et de culpabilité qui serait étroitement lié à la représentation sociale sexiste de la sexualité des femmes (Wolak et Finkelhor, 2016). L'étude de Wolak et Finkelhor (2016) menée auprès de 1631 victimes a également documenté plusieurs impacts sociaux découlant des actes de sextorsion, tels que la

perte de relation avec un.e ami.e, un.e partenaire ou un.e membre de la famille en lien avec l'agression et le vécu de difficultés à l'école et/ou au travail.

Vasiu et Vasiu (2020) ont examiné divers cas d'extorsion afin de documenter la nature des infractions et les conséquences vécues par les victimes. Les résultats montrent que les communications d'extorsion et de menaces, qu'elles soient de nature sexuelle ou non, peuvent perturber le fonctionnement habituel de la personne victime et positionner cette dernière dans un état de peur et de détresse. Elles peuvent également perturber les réactions et les interactions des personnes victimes et leur causer un préjudice social important, notamment par l'exposition de leurs informations personnelles (Vasiu et Vasiu, 2020). Selon une étude qualitative menée auprès de 18 femmes survivantes de PNCII, en plus de composer avec les conséquences délétères associées au partage non consensuel de contenu sexuel les impliquant, certaines d'entre elles ont aussi subi du harcèlement, de l'intimidation et des menaces de violence physique en provenance de leur agresseur ou agresseuse (Bates, 2017); l'utilisation malveillante des images intimes peut donc agir comme un catalyseur pour d'autres types de violence subséquente. À ce sujet, Holt et Ligget (2020) rapportaient que la moitié des victimes de PNCII avaient été victimes de ***doxxing***, c'est-à-dire que leurs informations personnelles (adresse, numéro de téléphone, lieu de travail ou d'étude, etc.) avaient été partagées avec leurs images intimes, augmentant leur risque d'être victime d'attaques et/ou d'abus subséquents. Considérant que l'arrêt des menaces ou des communications d'extorsion est parfois conditionnel à l'envoi d'importantes sommes d'argent, les victimes font également face à de nombreux préjudices économiques (Vasiu et Vasiu, 2020).

Dans la lutte contre la sextorsion, il est impératif de reconnaître les impacts délétères de cette dernière sur les victimes, et ce, tant au niveau social que physique, psychologique, professionnel et économique. En plus des conséquences de la violence elle-même, les victimes peuvent subir de la stigmatisation en provenance de leur famille, de leurs ami.e.s, de leurs pairs, des forces de l'ordre et des professionnel.le.s œuvrant en santé et en services sociaux. Cette stigmatisation a de graves conséquences sur leur santé mentale (Aborisade, 2021), les rend moins susceptibles de dénoncer les actes subis (Call, 2021; Patchin et Hinduja, 2020) et nuit à leur processus de guérison (Hamilton-Giachritsis *et al.*, 2020). La peur et la méfiance à l'égard des autorités peuvent également constituer des obstacles importants au dévoilement; les victimes hésitant à porter plainte par peur du jugement ou de condamnation, ou encore en raison de l'incrédulité des proches face à leur situation, ou encore du manque de preuves (Mumporeze, Han-Jin et Nduhura, 2021; Palmer, 2015). Ces craintes ne sont pas sans fondements puisque plusieurs victimes ont rapporté avoir reçu des réactions négatives et méprisantes de la part de la police à la suite du dévoilement de leurs expériences d'abus (Patchin et Hinduja, 2020; Wolak et Finhelkor, 2016). Plusieurs victimes de sextorsion ont également déclaré avoir été condamnées et isolées socialement par leurs réseaux sociaux, ou encore avoir été tenues responsables de leur sort. Il est en outre impératif de se positionner contre le blâme des victimes et de promouvoir le soutien social afin d'accroître le bien-être des victimes et de leur permettre de contrer les conséquences délétères de la sextorsion (Aborisade, 2021; Call 2021; Carlton, 2019; Hamilton-Giachritsis, *et al*., 2020; 2021; Mandau, 2021).

5. RECOURS POUR LES VICTIMES

5.1. Au niveau juridique

Les victimes décidant de poursuivre un sextorqueur ou une sextorqueuse font face à de nombreuses incohérences dans le traitement judiciaire des cas de sextorsion par les tribunaux. Aux États-Unis, comme au Canada, aucune loi ne criminalise la sextorsion pour les victimes adultes (Wittes *et al*., 2016). Aux Etats-Unis, la sextorsion est souvent classifiée en tant que pédopornographie (18 U.S.C. § 2251 ou 18 U.S.C. § 2252) ou, dans le cas de victimes adultes, en tant qu'extorsion générale (18 U.S.C. § 875(d)). Cependant, réduire les actes de sextorsion à de l'extorsion simple fait l'objet de critiques; outre le fait que l'aspect sexuel de l'abus ou de la violation de la vie privée soit occulté, la peine maximale pour des actes d'extorsion est de deux ans, ce qui s'avère particulièrement clément en réponse à des actes de sextorsion (Carlton, 2019). Cela contraste avec les lois sur la pédopornographie, qui prévoient des peines allant de cinq ans à la perpétuité, car elles peuvent être aggravées par des abus sexuels, des récidives, et les images violentes ou sadiques (18 U.S.C. § 2251 (2018); 18 U.S.C. § 2252 (2018)).

En pratique, les cas de sextorsion sont judiciarisés à travers une panoplie d'autres articles pénaux, y compris, mais sans s'y limiter, la diffamation, le voyeurisme, le harcèlement, les crimes haineux, le chantage, l'accès non autorisé à un ordinateur, l'envoi de communications dans l'intention d'affliger ou d'angoisser le ou la destinataire, l'extorsion, la pédopornographie et le piratage informatique (Hong *et al.*, 2020; Mania, 2020; McGlynn *et al*., 2017; Wittes *et al*., 2016). Cependant, ces lois comportent souvent des dispositions qui ne couvrent pas tous les actes prenant place au sein d'une dynamique de sextorsion, laissant les victimes avec moins de possibilités de recours (Henry et Flynn, 2019). Par exemple, l'article punissant le voyeurisme à New York (NYSL. § 250.45, 250.50, 250.55, 250.60) exclut les évènements où la photo a été prise et partagée par la victime de manière consensuelle, puis utilisée par la suite par l'auteur.e pour faire chanter la victime (Mania, 2020). De plus, cet article de loi portant sur le voyeurisme sexuel exige que la victime prouve que l'agresseur ou l'agresseuse était motivé.e par un désir de plaisir sexuel (Aborisade, 2021; Henry et Flynn, 2019). Cependant, tel que mentionné par Henry et ses collègues (2017), de nombreuses autres motivations peuvent être à la source de la sextorsion, telles que la volonté de prouver son statut social à ses pairs. Conséquemment, cet article de loi punissant le voyeurisme sexuel ne pourrait être systématiquement invoqué afin de condamner des actes de sextorsion. De façon similaire, de nombreuses lois aux États-Unis visant à punir la diffusion d'images intimes sont adaptées afin de condamner différentes manifestations de PNCII, mais excluent de nombreux cas de sextorsion (Wittes *et al*., 2016). Par exemple, les sextorqueurs et sextorqueuses ne mettront pas nécessairement à exécution leurs menaces de publication du contenu, car cela peut attirer l'attention et augmenter le risque d'être identifié.e.s par les forces de l'ordre (Açar, 2016).

Toujours aux États-Unis, les lois diffèrent d'un État à l'autre. Par conséquent, les résultats de poursuites judiciaires peuvent être très variables (Wittes *et al*., 2016). Une étude menée aux États-Unis rapporte que la durée des peines pour les auteur.e.s de sextorsion varie considérablement, soit de sept mois à 139 ans (Hong *et al*., 2020). En 2017, l'Utah a été le premier État à adopter une loi qui criminalise spécifiquement la sextorsion (Utah Code § 76-5b-204(2) (2017)). Toutefois, cette dernière a été particulièrement critiquée puisqu'elle exclut les cas où la sextorsion est motivée par un gain financier (Carlton, 2019). Inspirés par l'Utah,

26 autres États ont ensuite adopté de nouvelles lois afin de condamner la sextorsion. En ce qui concerne la manière dont les États devraient légiférer en matière de sextorsion, il existe différentes écoles de pensée. Certaines soutiennent que les caractéristiques propres à la sextorsion, distinctes de l'extorsion et du PNCII, font en sorte que celle-ci mérite des lois distinctes. Il a également été suggéré que les États pourraient incorporer l'élément de menace et de chantage de sextorsion dans les lois existantes sur la PNCII afin d'en faciliter la promulgation. Il pourrait également être nécessaire de distinguer les crimes au cours desquels le processus de condamnation est ajouté à des peines aggravées. Cette approche réduit la probabilité que l'auteur.e du crime soit acquitté.e en raison d'un détail technique. Une autre école de pensée serait de traiter les actes de sextorsion par l'entremise des articles de loi qui condamnent les actes d'extorsion. Cependant, comme mentionné précédemment, les sanctions sont particulièrement clémentes à l'égard de l'extorsion. Comme dans d'autres cas de violence à caractère sexuel, l'inadéquation entre la gravité du crime et la sévérité de la sanction peut décourager les victimes de faire appel à la justice. En effet, le coût émotionnel d'une telle procédure (souvent appelé « deuxième agression ») ne vaudrait pas la sanction pénale (Patchin et Hunduja, 2020). En outre, Henry, Flynn et Powell (2018) soulignent que de nombreuses victimes ne peuvent pas couvrir les frais de procédure judiciaire. Tant et aussi longtemps que ces barrières financières ne seront pas outrepassées et que les lois ne seront pas ajustées pour donner aux victimes une réelle chance d'obtenir un recours, les actes de sextorsion seront sous-déclarés.

En ce qui concerne le Canada, la législation entourant la sextorsion est similaire à celle des États-Unis. En règle générale, les politiques et les stratégies sociales et légales adoptées en société, notamment en ce qui concerne le PNCII, sont réactives plutôt que préventives. En effet, les législations, les pratiques juridiques et les programmes de prévention émergent en décalage à l'augmentation des cas de cyberdélinquance (Li, 2017). Au Canada, le projet de loi sur la protection des canadiens contre la cybercriminalité a été proposé en 2014. Il tente de pallier le besoin de gérer adéquatement les cas de cyberintimidation et apparaît en réponse directe au suicide d'une adolescente victime du partage des images de son agression sexuelle, l'affaire Rehthaeh Parsons. Le projet de loi C-13 sur la protection des canadiens contre la cybercriminalité a permis l'ajout d'une infraction d'ordre sexuel au Code criminel (2014) qui cible le partage non consensuel d'images intimes. L'article 162.1(1) punit

> Quiconque sciemment publie, distribue, transmet, vend ou rend accessible une image intime d'une personne, ou en fait la publicité, sachant que cette personne n'y a pas consenti ou sans se soucier de savoir si elle y a consenti ou non (…). (art. 162.1(1))

L'année suivant l'ajout de l'article, on enregistre une augmentation drastique des infractions d'ordre sexuel (MSP, 2021). Outre les articles de loi portant sur le PNCII, soit la publication, distribution, transmission ou vente d'images intimes non consensuelles (Code criminel, R.S.C., 1985, c. C-46 (article 162.1)), il existe des lois fédérales qui criminalisent l'extorsion de manière plus générale (Code criminel, R.S.C., 1985, c. C-46 (article 346)), et la pédopornographie (Code criminel, R.S.C., 1985, c. C-46 (Section 163.1)). Cependant, aucune de ces lois n'englobe entièrement la sextorsion; les lois sur l'extorsion ne comportent pas l'élément sexuel, et les lois sur les images intimes non consensuelles ne comportent pas d'élément de menace et/ou de chantage. De même, à l'instar des lois américaines, les lois sur le

voyeurisme au Canada n'incluent pas les cas où la photo a été prise par la victime elle-même. Ainsi, force est d'admettre que les personnes victimes de sextorsion sont très peu soutenues au niveau juridique (O'Malley et Holt, 2022; Wolak et Finkelhor, 2016). Par conséquent, comme aux États-Unis, les lois actuelles devraient être modifiées pour inclure les éléments qui sont propres à la sextorsion, ou de nouvelles lois devraient être adoptées pour criminaliser spécifiquement la sextorsion.

5.2. Au niveau de la santé et des services sociaux

Considérant que la sextorsion n'est pas reconnue socialement et légalement en tant que crime à part entière, présentant des dynamiques et des caractéristiques spécifiques, peu de ressources existent afin de répondre aux besoins des personnes qui en sont victimes. Lorsque ces dernières souhaitent recevoir des services de soutien psychologique, bien qu'elles puissent se tourner vers des organismes venant en aide aux victimes de violence à caractère sexuel, les personnes œuvrant au sein de ces organismes se disent peu outillées face à ce crime sexuel se trouvant à l'intersection de la technologie et la sexualité[12]. Devant leur manque de connaissances d'outils propres à la sextorsion, certain.e.s professionnel.le.s offrant des services d'aide accompagnent les victimes de cyberviolence de la même façon que celles ayant été victimes de violences à caractère sexuel dans le monde physique, occultant les besoins, les dynamiques et les conséquences particulières et propres à la cybervictimisation. Il importe aussi de mentionner que les victimes de sextorsion ne peuvent pas demander d'indemnisation pour soutien psychologique, puisque n'étant toujours pas reconnue comme un crime, la sextorsion n'est pas couverte par la loi de l'IVAC (indemnisation des victimes d'actes criminels). En effet, les seuls crimes apparentés à la sextorsion inclus au sein de ce programme sont le leurre informatique et la pornographie juvénile, offrant seulement de l'aide financière aux victimes mineures.

6. PERSPECTIVES DE GENRE SUR LA SEXTORSION

Bien que les recherches empiriques démontrent une surreprésentation des femmes et des personnes non binaires en tant que victimes, et des hommes en tant qu'auteurs de sextorsion, il est possible de croire que les pourcentages de femmes autrices de sextorsion et d'hommes victimes soient en réalité plus élevés. En effet, plusieurs études scientifiques ont documenté que les hommes étaient moins susceptibles de signaler les violences à caractère sexuel qu'ils ont subies (Allen, Ridgeway, et Swan, 2015; Young, Pruett et Colvin, 2018). En effet, la victimisation des hommes est peu reconnue socialement, voire tabou, et de nombreux hommes victimes ont le sentiment qu'il n'existe pas de ressources pour leur venir en aide. Cependant, bien que les victimes de sextorsion puissent être de toute identité de genre, les femmes et les personnes de la diversité de genre sont affectées de manière différente que les hommes par les violences à caractère sexuel. Selon certain.e.s auteur.e.s, les impacts psychologiques et sociaux du partage d'une image intime sont perçus comme plus négatifs, nuisibles et pénibles pour les femmes (Hasinoff et Shepherd, 2014; Henry et Powell, 2015; Powell et Henry, 2016). En effet, le potentiel de nuire à la réputation d'une femme par le biais d'une image sexuelle est si puissant que même les rumeurs de son existence peuvent inciter au harcèlement et à d'autres victimisations (Sales, 2016). Alors que la nudité masculine est plus

[12] Les données de cette section sont tirées d'entrevues semi-dirigées effectuées auprès de personnes travaillant dans le milieu de l'intervention en prévention et traitement des violences à caractère sexuel.

communément considérée comme drôle ou humoristique, bien qu'embarrassante, elle ne suscite pas la même hostilité de la part des pairs, tous genres confondus (Ringrose, Regehr et Whitehead, 2021). L'appropriation du corps des femmes par les hommes est illustrée par les menaces et le harcèlement envers les personnes dont les informations personnelles ont été publiées avec leurs photos intimes sans leur consentement. Ce type d'attaques est intrinsèquement lié au genre, les femmes étant nettement plus susceptibles d'être la cible de ces *cybermobs* (Salter et Crofts, 2015). La haine et la violence en ligne peuvent également se répercuter dans le monde physique, laissant de nombreuses victimes dans un état de peur et d'hypervigilance permanent (Citron et Franks, 2014; Holt et Ligget, 2020).

La perpétration d'agressions sexuelles et les conséquences qui en découlent trouvent leur source dans les dynamiques sexistes et patriarcales. Développée par DeKeseredy en 1988, la théorie du soutien des pairs masculins défend l'idée que la violence envers les femmes est entre autres légitimée par la création de liens et le partage de ressources, de croyances et de valeurs sexistes entre hommes présentant des idées toxiques. Ces croyances et ces valeurs seraient également reflétées, amplifiées et validées par d'autres figures masculines qui agissent à titre de modèles, ainsi que par les médias et par la pornographie mainstream. Selon plusieurs auteur.e.s, la pornographie mainstream, qui dépeint une image soumise des femmes et qui présente des rapports sexuels brutaux et dégradants serait liée à l'occurence de violence physique dans les relations hétérosexuelles à long terme et à des cas d'agression sexuelle lorsque les partenaires se séparent ou se divorcent (Bergen et Bogle, 2000; DeKeseredy et Corsianos, 2016; DeKeseredy, Dragiewicz, et Schwartz, 2017; DeKeseredy et Schwartz, 2009). La banalisation de la violence sexuelle à l'égard des femmes est également illustrée par la popularité du terme de recherche « *revenge porn sex* », générant plus de 2 730 000 résultats sur Google en 2016 (DeKeseredy et Schwartz, 2016).

Il est également possible d'analyser le phénomène de la violence à caractère sexuel basée sur l'image à travers le concept de l'homosocialité. Popularisé par Eve Kosofsky Sedgwick en 1985, ce concept défend l'idée que les liens entre pairs masculins hétérosexuels se construisent en opposition à l'homosexualité et à tout ce qui est typiquement associé au genre féminin. Plus précisément, Sedgwick décrit l'homosocialité en tant que dynamique triangulaire dans laquelle les femmes servent d'intermédiaires afin d'entretenir les liens non sexuels entre hommes. Selon cette idée, le partage non consensuel d'images intimes, obtenues dans un cadre consensuel ou non, à ses homologues masculins serait effectué dans le but de leur plaire, d'impressionner ou encore de prouver l'existence de conquêtes féminines. Au niveau empirique, l'étude de Henry et Flynn (2019) appuie d'ailleurs le concept d'homosocialité; les auteur.e.s ont documenté que le PNCII était plus souvent motivé par la gratification sexuelle et le désir de plaire à un réseau de pairs masculins que par la vengeance contre un.e ancien.ne partenaire. De la même manière, la sextorsion peut être utilisée pour la construction et la performativité de la masculinité.

7. OUTILS DE PRÉVENTION ET DE SENSIBILISATION

À ce jour, au Québec, les outils de prévention et les campagnes de sensibilisation qui concernent la sextorsion tendent à fournir une définition incomplète du phénomène, notamment en mentionnant uniquement la menace de partager les images intimes d'une personne mineure. Bien que la vulnérabilité des jeunes face à la sextorsion ne puisse être contestée, ce genre de définition pourrait contribuer à invisibiliser les adultes qui ne sont pas à l'abri de ce type d'abus.

Les campagnes de prévention existantes véhiculent principalement un discours responsabilisant les victimes, et diabolisant les formes d'expression et de communication sexuelle facilitées par la technologie, occultant par ailleurs la complexité du phénomène de sextorsion. Par exemple, le Centre canadien de la protection de l'enfance utilise l'expression « autoexploitation juvénile » pour désigner le sextage, laissant ainsi supposer qu'il est impossible de consentir à cette pratique sexuelle. La campagne #SnapToiPas du Servide ce Police de la Ville de Québec qui mobilise des slogans tels que « Même s'il te fait la baboune snap pas ta noune » (Figure 1) est également basée sur la négation de l'agentivité sexuelle des jeunes et des adolescent.e.s.

Figure 1: visuel de la campagne #SnapToiPas du Service de Police de la Ville de Québec

Malgré les bonnes intentions visant à contrer les violences à caractère sexuel en ligne, ces campagnes contribuent à la stigmatisation du sextage et tendent à identifier cette pratique en tant que cause d'une victimisation sexuelle basée sur l'image. Par exemple, la campagne #FullCélèbre (Figure 2) du Gouvernement du Canada fait une simple énumération « Ados, Sextos, Bobos » (Figure). Dans le but de contrer les violences basées sur l'image, il importe de renverser le narratif qui cible l'échange de sextos comme source du problème et de condamner l'abus et l'absence de consentement. Qui plus est, ce type de campagnes de sensibilisation à la sextorsion ou aux PNCII utilisent la peur comme levier de prévention, en mettant notamment l'accent sur la permanence du contenu en ligne, ainsi que sur les conséquences émotionnelles (culpabilité, tristesse), sociales (rejet, intimidation) et criminelles (accusation de pornographie juvénile) du partage d'images intimes.

Figure 2: visuel publicitaire de la campagne #FullCélèbre du Gouvernement du Canada

Figure 3: visuel de la campagne Full célèbre

À ce jour, au Québec, la principale solution proposée par les instances gouvernementales pour contrer la sextorsion est l'abstinence. Cette approche participe à la numérisation de la culture du viol, en faisant porter aux personnes victimes la responsabilité de l'abus subi (Dodge, 2015). Qui plus est, les discours véhiculés au sujet du sextage entretiennent une vision binaire, hétéronormative et simpliste du problème; l'accent étant mis sur la naïveté des filles qui partagent une image à leur partenaire masculin, plutôt que de se concentrer sur la notion de consentement et d'encourager une utilisation saine des technologies (Mercier, 2018; Powell et Henry, 2014). Cette dynamique met en exergue le besoin urgent de développer des campagnes de sensibilisation axée sur la sexualité positive pour prévenir les violences à caractère sexuel en ligne (Mercier, 2018). Finalement, il importe de développer des campagnes de prévention qui abordent le phénomène de la sextorsion dans sa globalité, et non seulement les évènements de menace de partage d'images intimes.

8. CONTRER LA SEXTORSION : RECOMMANDATIONS ET PISTES DE SOLUTION

8.1. Vers une redéfinition de la sextorsion

Afin de considérer le vaste continuum des actes de sextorsion, nous proposons une définition élargie du phénomène.

> **La sextorsion est une forme d'extorsion de nature sexuelle par laquelle une personne tente d'obtenir quelque chose tel qu'une image intime, une faveur sexuelle ou tout autre avantage, sans le libre consentement de la personne concernée, par diverses techniques de manipulation ou par l'emploi de menaces.**

Cette définition permet de conceptualiser la sextorsion en tant qu'acte de violence sexuelle et de considérer le phénomène au-delà de la menace du partage d'images intimes. Cette définition permet également de mettre en exergue un vaste éventail de comportements puisqu'elle inclut tout évènement d'extorsion lié à la sexualité, que ce soit au niveau du type de contenu, du chantage ou de ce que l'on tente de soutirer à la victime. Finalement, cette définition permet de considérer autant les évènements de cybersextorsion que les évènements de sextorsion qui prennent place dans le monde physique, notamment dans les milieux de travail ou au sein des instances gouvernementales.

8.2. Vers un changement de vision dans la lutte contre la sextorsion

Tel que soulevé précédemment (voir section 4), les victimes font face à de multiples jugements lorsque vient le temps de chercher de l'aide, notamment de la part de divers.es professionnel.le.s œuvrant en santé et en services sociaux (intervenant.e psychosocial.e ou communautaire, avocat.e et forces de l'ordre). De plus, certain.e.s professionnel.le.s sous-estiment les impacts du crime en raison de l'absence de contact physique entre la victime et l'agresseur ou agresseuse (Martin et Slaine, 2015; Palmer, 2015). Les impacts émotionnels et psychologiques de la sextorsion sont souvent jugés moins graves que les agressions sexuelles physiques, bien que des études montrent que les victimes des deux crimes subissent des niveaux similaires de dommage (Hamilton-Giachritsis *et al*., 2020).

Nous proposons deux pistes de solution pour faciliter un environnement sécure, adapté et propice au dévoilement et au traitement pour les victimes de sextorsion :

1. **L'ensemble de la population doit être sensibilisée aux enjeux liés à la sextorsion afin d'accroître l'empathie accordée aux victimes, lutter contre le blâme porté aux victimes (*victim-blaming*) et améliorer les services offerts à ces dernières.**
2. **Les intervenant.e.s œuvrant auprès des victimes de sextorsion doivent recevoir de l'éducation et de la formation professionnelle adaptée, fiable et éprouvée afin que les victimes disposent de ressources bienveillantes et adaptées à leurs besoins.**

8.3. Importance de l'éducation et la formation professionnelle

Tel que mentionné précédemment, les intervenant.e.s indiquent manquer de confiance et de recours appropriés pour intervenir dans un contexte de cybervictimisation sexuelle, et estiment que des formations supplémentaires sont nécessaires pour répondre aux besoins des victimes (Martin et Slaine, 2015). Dans le cadre de notre recension, nous avons effectué des entrevues exploratoires auprès d'intervenant.e.s qui accompagnent des victimes de violence à caractère sexuel, et ces dernières ont explicitement nommé le besoin de formation sur les spécificités de la victimisation sexuelle en ligne pour mieux répondre à leurs besoins. Parmi les défis auxquels les intervenant.e.s sont confronté.e.s, citons l'augmentation du nombre de cas dans les dernières années, la gravité du préjudice que le cas doit présenter avant que l'intervention ne soit menée par les forces de l'ordre, le manque de suivi auprès des victimes et le manque d'outils, de modèles et de ressources adaptés à la spécificité de ce type de violence (Martin et Slaine, 2015).

Il est clair que des formations sont nécessaires et doivent être adaptées aux différent.e.s intervenant.e.s et groupes d'intérêt en matière de sextorsion, notamment les instances politiques, les forces de l'ordre, les professionnel.le.s de la santé et des services sociaux, les corps enseignants, le milieu étudiant, les parents, les médias, le grand public, et plus encore. Certains articles académiques ont suggéré des interventions qui mettent l'accent sur les victimes potentielles pour leur apprendre des techniques de cybersécurité, d'autoprotection et d'éducation en cas de victimisation (Açar, 2016; Kopecký, 2017; Vasiu et Vasiu, 2020). Cependant, d'autres auteur.e.s ont critiqué cette approche considérant qu'elle fait porter aux

individus la responsabilité de ne pas vivre de cyberviolence sexuelle (Aborisade, 2021; Hamilton-Giachritsis *et al*., 2020; Mandau, 2021; Wolak, Finkelhor, Walsh et Treitman, 2018). Ces dernier.e.s proposent plutôt que les outils et formations, telles que des campagnes de sensibilisation du public et des ateliers éducatifs, visent les auteur.e.s du crime. En particulier, les personnes qui élaborent ces outils et formations devraient se concentrer davantage sur la moralité sous-jacente au partage de contenu intime sans le consentement, sur la responsabilité des spectateurs et sur la remise en question des attitudes de blâme envers les victimes. Henry, Flynn et Powell (2020) défendent également l'importance d'aborder au sein de formations professionnelles les façons dont certaines populations marginalisées (les personnes autochtones, les personnes de la diversité sexuelle et de genre, les personnes en situation de handicap, les personnes de la diversité culturelle, etc.) sont différemment touchées par la sextorsion et les obstacles supplémentaires qu'elles peuvent rencontrer.

Selon Vasiu et Vasiu (2020), il est aussi nécessaire de former des équipes spécialisées pour détecter les menaces de sextorsion à un stade précoce, d'améliorer le partage d'informations entre les différents acteurs et actrices impliqué.e.s dans les solutions, de développer des lignes directrices pour les agent.e.s chargé.e.s de l'application de la loi et d'améliorer le code civil pour répondre de manière plus appropriée aux cas de sextorsion. De plus, davantage de financement devrait être accordé aux groupes qui étudient des aspects connexes à la sextorsion, tels que les inégalités structurelles et la haine en ligne. Joignant leurs voix à plusieurs autres auteur.e.s, Vasiu et Vasiu (2020) soulèvent l'importance de la sensibilisation et de l'éducation notamment en matière de cyber-risques, de la conservation des preuves numériques, des réactions à privilégier face à ce type d'infraction et du signalement des incidents de sextorsion aux autorités.

8.4. Responsabilités de l'industrie technologique

Les corps policiers sont confrontés à plusieurs défis lorsqu'ils enquêtent sur des cas de sextorsion, liés notamment aux frontières juridictionnelles et aux difficultés à récolter la preuve (Flynn et Henry, 2019). Les opérations préventives visant à identifier les personnes agresseuses permettent de réduire les abus futurs. Parmi les moyens pour y parvenir, citons les opérations d'infiltration en ligne, la surveillance et l'investigation des cyberespaces. Cependant, comme le souligne Açar, (2016), Internet est devenu trop vaste pour pouvoir être adéquatement surveillé, compte tenu des ressources limitées des corps policiers. Le fardeau de la preuve est donc un défi difficile à surmonter. Même lorsque la publication non consensuelle d'une image est retracée jusqu'à un appareil, la facilité avec laquelle l'appareil peut être accédé par autrui ou piraté rend difficile la preuve, hors de tout doute raisonnable, que le ou la propriétaire de l'appareil est nécessairement la personne ayant publié l'image (Henry, Flynn et Powell, 2020).

La nature des crimes facilités par la technologie pose des défis spécifiques en matière de détection, d'arrestation et de poursuite policière. Par exemple, les auteur.e.s de ces crimes peuvent utiliser plusieurs outils pour dissimuler des informations d'identification, comme le cryptage, les réseaux privés virtuels (VPN), les serveurs proxy, ainsi que le stockage « en nuage » qui leur permet de sauvegarder et d'accéder à des contenus illégaux sans en avoir la possession à leur domicile (Henry et Witt, 2021; Ministère de la Justice, 2017). En outre, la mondialisation

de la sextorsion induit qu'elle est devenue une menace imminente tant pour les *sexters* qui produisent du contenu que pour toute autre personne pouvant être potentiellement victime de création non consensuelle d'images intimes (p. ex. *deepfake* ou vidéovoyeurisme) puisque l'accès des abuseurs et abuseuses aux victimes potentielles est facile, rapide, vaste et persistant (Dodge et Spencer, 2018; Hamilton-Giachritsis *et al*., 2020; Henry et Flynn, 2019). En effet, cette mondialisation permet aux auteur.e.s d'infraction de former des réseaux organisés pour collecter du matériel explicite à caractère sexuel illégal, ainsi que pour partager des connaissances sur des manières d'échapper aux forces de l'ordre. Par conséquent, il est primordial de renforcer la coordination mondiale entre les différentes agences d'application de la loi, notamment en facilitant l'échange de preuves entre les juridictions étrangères lorsqu'un crime traverse les frontières étatiques.

L'industrie technologique peut également jouer un rôle non négligeable dans la cybercriminalité. Leurs plateformes étant un vecteur de sextorsion, les entreprises technologiques ont la responsabilité de contribuer à sa prévention et à sa répression. Une étude de De Angeli, Falduti, Menendez Blanco et Tessaris (2021) a analysé la facilité avec laquelle les internautes peuvent signaler une image partagée sans le consentement de la personne y figurant. Sur les 45 plateformes de leur échantillon, seules 24 disposaient d'une fonction de signalement d'une image ou d'une vidéo. Huit sites Internet proposaient aux utilisateurs et utilisatrices un champ de texte vide pour décrire leur plainte, neuf offraient l'option générique « signaler un abus » et seulement sept proposaient une option spécifique pour signaler la *revenge porn*. En outre, certains processus de déclaration s'avéraient laborieux. L'incapacité de signaler ou la difficulté de signaler ainsi que le manque de spécificité des méthodes de signalement des abus sont autant d'obstacles pour les victimes. Finkelhor et Wolak, du Centre de recherche sur le crime contre les enfants ont notamment souligné la nécessité de faciliter le retrait des contenus en ligne (Finkelhor et Wolak, 2020).

Selon Vasiu et Vasiu (2020), afin de contrer la sextorsion, il est fondamental de documenter les échanges entre les victimes et les personnes agresseuses, soit l'initiation des interactions, le déroulement de ces dernières et l'intensification des communications de sextorsion. En effet, le développement d'outils d'analyse textuelle permettrait d'améliorer la prévention, et ce, en prédisant et en identifiant de manière plus efficace les tactiques de chantage. Le développement de logiciels avancés permettrait non seulement de filtrer ces échanges, mais également de les révoquer et de les acheminer aux autorités légales. La prise en charge de ce type d'infraction serait ainsi beaucoup plus rapide et efficace (Vasiu et Vasiu, 2020). Hong et ses collègues (2020), pour leur part, ont suggéré que les entreprises développent des systèmes d'intelligence artificielle (IA) pour détecter la sextorsion et mettre en place des réseaux de soutien pour les victimes. Ce type de recommandation a également été fait dans le cadre de développement d'applications et de jeux (Palmer, 2015). Cependant, les systèmes d'IA sont limités et doivent être utilisés en complément des ressources humaines. Açar (2016) a recommandé aux parents d'installer des logiciels de surveillance et de blocage supplémentaires qui pourraient réduire davantage le risque de victimisation de leur enfant. Henry et Witt (2021) suggèrent, quant à eux, l'intégration de cache-caméra sur tous les appareils ainsi que l'obligation pour tout site Internet, nécessitant la création d'un compte, d'exiger des mots de passe forts et une authentification à deux facteurs (un processus qui exige deux étapes pour se connecter à un compte). Facebook a aussi proposé une solution : en utilisant PhotoDNA (autrement connu

sous le nom *hashing* ou *digital fingerprinting*) les victimes ou potentielles victimes peuvent télécharger de manière préalable les images qu'elles craignent de voir publiées en ligne. Un système d'IA pourrait alors détecter et bloquer toute tentative de télécharger une image similaire. Facebook s'est également engagé à désactiver les comptes des contrevenant.e.s qu'il détecte (Henry, Powell et Flynn, 2017). Bien qu'il s'agisse d'une idée créative, la victime potentielle doit être à l'aise de confier ses images intimes à Facebook. Il faut également que les victimes soient conscientes de l'existence de l'image en question et en possession de l'image utilisée contre elles, ce qui n'est pas toujours le cas. De plus, dans le cadre d'une modification mineure de l'image, le système peut complètement être contourné (Henry et Witt, 2021).

Les entreprises technologiques peuvent également avoir un impact positif sur la lutte contre la sextorsion en éduquant leurs utilisateurs et utilisatrices et en intégrant du matériel éducatif sur leurs plateformes. De plus, les détaillants pourraient fournir du matériel éducatif lors de la vente des appareils électroniques (Palmer, 2015). De même, les entreprises technologiques qui possèdent des moteurs de recherche, tels que Google ou Yahoo, auraient la possibilité de rendre les ressources de prévention et de récupération facilement accessibles en les plaçant plus haut dans les résultats de recherche (Palmer, 2015).

Des politiques de suppression d'images sexuelles non consensuelles sont déjà en place pour la plupart des plateformes d'hébergement de contenu grand public. Par exemple, Google, Microsoft, Twitter et Meta (qui comprend Facebook et Instagram) ont tous mis en place des politiques de retrait d'image. Toutefois, Google aurait bloqué un projet de loi à New York qui visait à faire du PNCII un délit et aurait permis aux victimes de poursuivre les plateformes d'hébergement pour faire retirer les images et qui aurait protégé les potentielles victimes (Conley et Fonrouge, 2018). Force est d'admettre qu'il existe un intérêt pour le trafic généré par les images intimes non consensuelles et les gains financiers qui y sont associés. En effet, il existe des sites qui cherchent spécifiquement à héberger ce type de contenu. En 2010, l'Américain Hunter Moore a mis en ligne le site *Is Anyone Up?*, où la majorité des images intimes étaient publiées sans consentement, et tapissées de commentaires dégradants. Lorsqu'il était actif, le site attirait plus de 300 000 visites par jour et générait jusqu'à 30 000 $ de revenu par mois. En entrevue, Hunter Moore se déresponsabilise, affirmant que les personnes n'auraient d'emblée pas dû partager d'image intime, se présentant même en « sauveur » de l'Internet et en se félicitant d'avoir appris aux victimes une leçon de cybersécurité (Morris, 2012). Bien que ce site ne soit plus actif, il existe encore à ce jour des pages dédiés aux PNCII. D'ailleurs, une analyse de contenu sur un site dédié au PNCII montrait que le trafic moyen sur les images dépassait les 5 000 vues et on estime que les chiffres réels sont plus élevés en raison de la possibilité d'enregistrer une copie des photos (Uhl *et al.*, 2018). Pour arriver à retirer une image hébergée sur un site, il faut s'adresser au propriétaire du domaine. Malheureusement, ce processus peut être compliqué puisque les images sont fréquemment publiées sur plus d'un site et bien souvent, les demandes de retrait sont ignorées. À ce sujet, en Australie, une législation qui habilite les tribunaux à tenir les coupables responsables du retrait, de la suppression et de la destruction du contenu dans un délai de 48 heures a été adoptée. Tout manquement à cette obligation peut entraîner une peine maximale de deux ans d'emprisonnement (Henry, Flynn et Powell, 2018). Une telle législation devrait être étendue aux fournisseurs de services Internet, aux moteurs de recherche et aux plateformes d'hébergement de contenu.

CONCLUSION

Dans ce rapport, nous avons passé en revue l'état actuel de la littérature académique sur la sextorsion et autres formes de violence à caractère sexuel connexes, en soulignant les données en ce qui a trait aux victimes, aux auteur.e.s, aux contextes, ainsi qu'aux recours et ressources qui existent actuellement pour faire face à la sextorsion. Nous soutenons qu'il est impératif de reconnaître les conséquences que la sextorsion engendre sans limiter l'agentivité sexuelle des individus. Nous formulons plusieurs recommandations pour un changement au niveau professionnel, industriel, juridique et politique. Une concertation de chercheuses, de chercheurs et de professionnel.le.s provenant de différentes disciplines et milieux est de mise pour s'attaquer au problème de façon plus active, et pour formuler des plans d'action interdisciplinaires qui tiennent en compte des victimes de sextorsion, et agissent directement pour prévenir les comportements menant aux gestes de violences sexuelles.

Les cas enregistrés de violences à caractère sexuel par et via Internet sont en augmentation. Bien que le phénomène ne soit pas nouveau, sa portée, sa nature, sa durée et ainsi que la protection légale offerte sont des sujets très peu étudiés. De cette manière, il apparaît important de mener des recherches dans le domaine des violences à caractère sexuel en ligne afin de développer des législations, des techniques de régulation et des programmes de prévention adaptés aux nouveaux outils numériques, utilisés pour poser des gestes de cyberviolence (Henri et Powell, 2018). En effet, la cybersextorsion risque de continuer à prendre de l'ampleur en raison des avancées technologiques, notamment au niveau du développement des technologies d'intelligence artificielle (p. ex. *deepfake*) et des techniques d'anonymisation en ligne (p. ex. paiement par bitcoin). Ainsi, la technologie semble à la fois la solution et le problème en termes de prévention de la sextorsion (Carlton, 2019).

Enfin, une collaboration internationale est nécessaire dans l'industrie technologique, ainsi qu'auprès des différentes instances policières et gouvernementales. En effet, la législation actuelle devrait être élargie, et de nouvelles lois devraient être adoptées pour prendre en compte les caractéristiques spécifiques de la sextorsion et garantir que les sanctions pénales s'arriment aux conséquences potentielles sur la victime. La gestion de la violence en ligne requiert le développement de stratégies innovantes et créatives. Finalement, nous croyons qu'il est nécessaire que des efforts concertés en recherche, action et législation soient mis en place afin d'approfondir les connaissances des instances politiques et de la société civile au sujet de ses manifestations autant dans l'univers technologique que dans le monde physique.

RÉFÉRENCES

Article de journaux

Agence France Presse. (2014, 11 février). La face sombre d'Internet utilisée par le crime organisé. *Le Devoir*. https://www.ledevoir.com/monde/399577/la-face-sombre-d-internet-utilisee-par-le-crime-organise

Cloutier, E. (2021, 31 mai). Explosion des cas de sextorsion au Québec. *Journal de Québec*. https://www.journaldequebec.com/2021/05/31/explosion-des-cas-de-sextorsion

Conley, K. et Fonrouge, G. (2018, 21 juin). Google Kills Revenge Porn Bill. *New York Post*.https://nypost.com/2018/06/21/new-yorks-revenge-porn-bill-dies-after-11th-hour-campaign-by-google/

Kari, S. (2010, 29 juillet). Sex Scandals Gets Immigration Judge 18 Month Jail Sentence. *National Post*. https://nationalpost.com/posted-toronto/sex-scandal-gets-immigration-judge-18-month-jail-sentence

Kelley, K. (2019, 19 mars). New Data on Sextortion: 124 Additional Public Cases. *Lawfare*. https://www.lawfareblog.com/new-data-sextortion-124-additional-public-cases

Lanney, T. (2021, 2 novembre). Le site de rencontre Atraf victime de chantage aux données. *Tetu*. https://tetu.com/2021/11/02/israel-hackers-black-shadow-vol-donnees-site-lgbt-rencontre-gay-atraf-rancon/

Morris, A. (2012, 13 novembre). Hunter Moore: The Most Hated Man on the Internet. *Rolling Stone*.https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/

Rivard, J. (2021, 20 mai). Les cas de sextorsion ont triplé chez les garçons de 12 à 17 ans cette année. *Radio-Canada*. https://ici.radio-canada.ca/nouvelle/1794917/sextorsion-prevention-sq-abitibi-temiscamingue

Russel, A. (2019, 23 juillet). Extortion Cases Increased 170% from 2012 to 2018 in Canada: StatCan. *Global News*.https://globalnews.ca/news/5672420/extortion-cases-increased-170-from-2012-to-2018-in-canada-statscan/

Schwartz, D. (2013, 13 août). The Fine Line Between 'Sexting'and Child Pornography. *CBC News*. https://www.cbc.ca/news/canada/the-fine-line-between-sexting-and-child-pornography-1.1367613

Slugosky, K. (2021, 9 mars). Child Luring and Sextortion Cases Online Spikes Since Start of Pandemic. *Global News*.https://globalnews.ca/news/7683360/covid-19-child-luring-sextortion-online-cases/

Somos, C. (2021, 9 février). Child's sextortion' Reports on the Rise During Pandemic: National Tip Line. *CTV New*s.https://www.ctvnews.ca/canada/child-sextortion-reports-on-the-rise-during-pandemic-national-tip-line-1.5302282

Articles académique

Aikens, M. (2016). *The Cyber Effect: An Expert in Cyberpsychology Explains How Technology Is Shaping Our Children, Our Behavior, and Our Values-and What We Can Do About It.* (1re éd.). Penguin Random House.

Aborisade, R. A. (2021). Image-Based Sexual Abuse in a Culturally Conservative Nigerian Society: Female Victims' Narratives of Psychosocial Costs. *Sexuality research and social policy*, 1-13.

Acar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, *10*(2).

Allen, C. T., Ridgeway, R. et Swan, S. C. (2015). College Students' Beliefs Regarding Help Seeking for Male and Female Sexual Assault Survivors: Even Less Support for Male Survivors. *Journal of Aggression, Maltreatment & Trauma*, *24*(1), 102-115.

Bates, S. (2017). Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology*, *12*(1), 22-42. https://doi.org/10.1177/1557085116654565

Bergen, R. K. et Bogle, K. A. (2000). Exploring the Connection Between Pornography and Sexual Violence. *Violence and Victims*, *15*(3), 227-234.

Bouchard, G.., Lussier, Y. (2006). Les relations assistées par ordinateur: Le profil des cybercouples. *Revue québécoise de psychologie*, *27*(2), 245-262.

Borrajo, E., Gámez-Guadix, M., Calvete, E. (2015). Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression. *Psychological reports*, *116*(2), 565-585.

Buhi, E. R., Blunt, H., Wheldon, C., & Bull, S. S. (2014). Sexuality and new technologies. Dans D. L. Tolman, L. M. Diamond, J. A. Bauermeister, W. H. George, J. G. Pfaus, & L. M. Ward (Eds), *APA handbook of sexuality and psychology, Vol. 2. Contextual approaches* (pp. 77–101). American Psychological Association

Call, C. (2021). Perceptions of Image-Based Sexual Abuse Among the American Public. *Criminology, Criminal Justice, Law & Society*, *22*(3), 30145.

Carlton, A. (2019). Sextortion: The Hybrid Cyber-Sex Crime. *North Carolina Journal of Law & Technology*, *21*(3), 177-216.

Citron, D. K. et Franks, M. A. (2014). Criminalizing Revenge Porn. *Wake Forest Law Review, 49*(347), 345–383.

Close, A. G., Zinkhan, G. M., Finney, R. Z. et Center, N. O. (2004). Cyber-Identity Theft: A Conceptual Model and Implications for Public Policy. Dans *Proceedings of the American Marketing Association Summer Educator's Conference*.

Code criminel canadien. (1985). Partie IX : Infractions contre les droits de propriété, Tiré de : https://laws-lois.justice.gc.ca/fra/lois/C-46/page-34.html#h-114950

Code criminel canadien, (2014). *Partie V : infractions d'ordre sexuel, actes contraires aux bonnes mœurs, inconduite.* Tiré de :

http://criminalnotebook.ca/index.php/Fran%C3%A7ais:Partie_V_-_Infractions_d%E2%80%99ordre_sexuel,_actes_contraires_aux_bonnes_moeurs,_inconduite

Cohen, L. E. et Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Association, 44*(4), 588-608. https://doi.org/10.2307/2094589

Crimes Amendment (Intimate Images) Act 2017 No 29 (NSW), amendement to the *Crimes Act 1900,* 27 june 2017. Tiré de: https://legislation.nsw.gov.au/#/view/act/2017/29

Crimes (Intimate Image Abuse) Amendment Act 2017, A2017-22 (ACT). Tiré de: https://www.legislation.act.gov.au/a/2017-22/20170830-67084/pdf/2017-22.pdf

De Angeli, A., Falduti, M., Menendez Blanco, M., et Tessaris, S. (2021). Reporting Revenge Porn: A Preliminary Expert Analysis. *CHItaly 2021: 14th Biannual Conference of the Italian SIGCHI Chapter*, 1-5. https://doi.org/10.1145/3464385.3464739

DeKeseredy, W. S. (1988). Woman Abuse in Dating Relationships: The Relevance of Social Support Theory. *Journal of Family Violence*, *3*(1), 1-13.

DeKeseredy, W. et Corsianos, M. (2015). Violence Against Women in Pornography (1re éd.). Routledge. https://doi.org/10.4324/9781315652559

DeKeseredy, W. S., Dragiewicz, M. et Schwartz, M. D. (2017). Abusive Endings. Dans *Abusive Endings*. University of California Press.

DeKeseredy, W. S. et Schwartz, M. (2009). Dangerous Exits. In *Dangerous Exits*. Rutgers University Press.

DeKeseredy, W. S. et Schwartz, M. D. (2016). Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory. *Sexualization, Media & Society*, 1-8. https://doi.org/10.1177/2374623816684692

Dilmac, J. A. (2017). Humiliation sur internet : nouvelle forme de cyberdéviance? *Déviance et société, 2*(41), 305-330. https://doi.org/10.3917/ds.412.0305

Dodge, A. (2015). Digitizing Rape Culture: Online Sexual Violence and the Power of the Digital Photograph. *Crime, Media, Culture, 12*. https://doi.org/10.1177/1741659015601173

Dodge, A., & Spencer, D. C. (2018). Online sexual violence, child pornography or something else entirely? Police responses to non-consensual intimate image sharing among youth. *Social & Legal Studies*, *27*(5), 636-657.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018a). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609-625.

Dragiewicz, M., Woodlock, D., Harris, B., & Reid, C. (2018b). Technology-facilitated coercive control. In *The Routledge international handbook of violence studies* (pp. 244-253). Routledge.

Drouin, M. et Tobin, E. (2014). Unwanted but Consensual Sexting Among Young Adults: Relations with Attachment and Sexual Motivations. *Computers in Human Behavior, 31*, 412-418. https://doi.org/10.1016/j.chb.2013.11.001

Eaton, A. A., Ramjee, D. et Saunders, J. F. (2022). The Relationship Between Sextortion During COVID-19 and Pre-Pandemic Intimate Partner Violence: A Large Study of Victimization among Diverse U.S Men and Women. *Victims & Offenders*, *0*(0), 1-18. https://doi.org/10.1080/15564886.2021.2022057

Eleuteri, S., & Terzitta, G. (2021). Sexuality during the COVID-19 pandemic: The importance of Internet. *Sexologies*, *30*(1), e55-e60.

Feigenblatt, H. (2020). *Breaking the Silence Around Sextortion: The Links Between Power, Sex and Corruption*. Transparency International. https://apo.org.au/node/278106

Felson, M. (1998). Crime and Everyday Life (2e éd.). Thousand Oaks, CA: Pine Forge Press.

Ferguson, G. (Ed.). (2022). *Global Corruption: Its Regulation Under International Conventions, US, UK, and Canadian Law and Practice* (Vol. 1). University of Victoria Libraries.

Fortin, F. et Desfachelles, M. (2019). Le sexting secondaire chez les adolescent·e·s origines et enjeux d'une source de cyberintimidation. *Déviance et société, 43*, 329-357. https://doi.org/10.3917/ds.433.0329

Garlick, S. (2011). A New Sexual Revolution? Critical Theory, Pornography, and the Internet. *Canadian Review of Sociology/Revue Canadienne de Sociologie*, *48*(3), 221-239. https://doi.org/10.1111/j.1755-618X.2011.01264.x

Geldenhuys, K. (2016). Sextortion-a new form of cybercrime. *Servamus Community-based Safety and Security Magazine*, *109*(8), 14-18.

Gendarmerie royale du Canada. (2015). *Stratégie de lutte contre la cybercriminalité*. Tiré de : https://www.rcmp-grc.gc.ca/fr/strategie-lutte-cybercriminalite-gendarmerie-royale-du-canada

Grubb, A. R., Brown, S. J., Hall, P. et Bowen, E. (2019). From "Sad People on Bridges" to "Kidnap and Extortion" : Understanding the Nature and Situational Characteristics of Hostage and Crisis Negotiator Deployments. *Negotiation and Conflict Management Research, 12*(1), 41-65. https://doi.org/10.1111/ncmr.12126

Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Alves-Costa, F., Pintos, A., Metcalf, T. et Beech, A. (2021). Technology Assisted Child Sexual Abuse: Professionals' Perceptions of Risk and Impact on Children and Young People. *Child Abuse & Neglect*, *119*, 104651.

Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Alves-Costa, F. et Beech, A. (2020). Technology Assisted Child Sexual Abuse in the UK: Young People's Views on the Impact of Online Sexual Abuse. *Children and Youth Services Review*, *119*, 105451.

Hasinoff, A. A. et Shepherd, T. (2014). Sexting in Context: Privacy Norms and Expectations. *International Journal of Communication*, *8*, 24.

Hassan, G. (2018). Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence. *International Journal of Developmental Sciences*, 12(1-2), 71-88.

Henry, N. et Flynn, A. (2019). Image-based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence against women*, *25*(16), 1932–1955. https://doi.org/10.1177/1077801219863881

Henry, N., Flynn, A. et Powell, A. (2018). Policing Image-based Sexual Abuse: Stakeholder Perspectives. *Police Practice and Research: An International Journal, 19(6)*, 565–581. https://doi.org/10.1080/15614263.2018.1507892

Henry, N., Flynn, A. et Powell, A. (2020). Technology-facilitated Domestic and Sexual Violence: A Review. *Violence against women*, *26*(15-16), 1828-1854.

Henry, N. et Powell, A. (2015). Embodied Harms: Gender, Shame, and Technology-facilitated Sexual Violence. *Violence Against Women, 21*(6), 758-779. https://doi.org/10.1177/1077801215576581

Henry, N. et Powell, A. (2015a). Beyond the 'Sext': Technlogy-facilitated Sexual Violence and Harassment Against Adult Women. *Journal of Criminology, 48*(1), 104-118. https://doi.org/10.1177/0004865814524218

Henry, N. et Powell, A. (2018). Technology-facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse*, *19*(2), 195–208. https://doi.org/10.1177/1524838016650189

Henry, N., Powell, A. et Flynn, A. (2017). Not Just 'Revenge Pornography': Australians' Experiences of Image-based Abuse. *A summary report.* Melbourne: RMIT University.

Henry, N. et Witt, A. (2021). Governing Image-Based Sexual Abuse: Digital Platform Policies, Tools, and Practices. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited.

Hill, R. (2015). Cyber-misogyny: Should Revenge Porn be Regulated in Scotland, and if so, How ?. *Scripted, 12*(2), 118-140.

Holt, T. J. et Bossler, A. M. (2007). Examining the Applicability of Lifestyle-routine Activities Theory for Cybercrime Victimization. *Deviant Behavior, 30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Holt, K., & Liggett, R. (2020). Revenge Pornography. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 1131-1149.

Hong, S., Lu, N., Wu, D., Jimenez, D. E. et Milanaik, R. L. (2020). Digital Sextortion: Internet Predators and Pediatric Interventions. *Current opinion in pediatrics*, *32*(1), 192-197.

Kelly, L. (1988). *Surviving Sexual Violence*. Cambridge : Polity Press.

Koch, R. et Miles, S. (2021). Inviting the Stranger in: Intimacy, Digital Technology and New Geographies of Encounter. *Progress in Human Geography*, *45*(6), 1379-1401. https://doi.org/10.1177/0309132520961881

Kopecký, K. (2017). Online Blackmail of Czech Children Focused on So-called "Sextortion"(Analysis of Culprit and Victim Behaviors). *Telematics and Informatics*, *34*(1), 11-19.

Lehmiller, J. J., Garcia, J. R., Gesselman, A. N. et Mark, K. P. (2021). Less Sex, but More Sexual Diversity: Changes in Sexual Behavior during the COVID-19 Coronavirus Pandemic. *Leisure Sciences*, *43*(1-2), 295-304. https://doi.org/10.1080/01490400.2020.1774016

Lenhart, A., Ybarra, M. et Price-Feeney, M. (2016). Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of Revenge Porn. *Data and Society*.https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Li, J. X. (2017). Cyber Crime and Legal Countermeasures: A Historical Analysis. *International Journal of Criminal Justice Sciences, 12*(2), 196-207. https://doi.org/10.5281/zenodo.1034658

Macilotti, G. (2019). Violence et humiliation à l'ère numérique : une étude en milieu scolaire. *Déviance et Société*, *43*(3), 299-328.

Mandau, M. B. H. (2021). "Snaps","Screenshots", and Self-blame: A Qualitative Study of Image-based Sexual Abuse Victimization Among Adolescent Danish Girls. *Journal of Children and Media*, *15*(3), 431-447.

Mania, K. (2020). The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective. *Sexuality & Culture*, *24*(6), 2079-2097.

Marcum, C. D. (2008). Identifying Potential Factors of Adolescent Online Victimization for High School Seniors. *International Journal of Cyber Criminology, 2*(2), 346-367.

Martin, J. et Slane, A. (2015) Child Sexual Abuse Images Online: Confronting the Problem. *Child & Youth Services, 36*(4), 261-266. https://doi.org/10.1080/0145935X.2015.1092828

McGlynn, C. et Rackley, E. (2017). Image-Based Sexual Abuse. *Oxford Journal of Legal Studies*, *37*(3), 534-561. https://doi.org/10.1093/ojls/gqw033

McGlynn, C., Rackley, E. et Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-based Sexual Abuse. *Feminist Legal Studies, 25*, 25-46. https://doi.org/10.1007/s10691-017-9343-2

Mercier, É. (2018). Humiliation, responsabilisation et moralisation dans les discours sur le partage d'images intimes chez les jeunes. *Revue Jeunes et Société, 3*(1), 56-77.

Mesch, G. S. (2009). Parental mediation, online activities and cyberbullying. *CyberPsychology and Behavior*, *12*(4), 387-393. https://doi.org/10.1089/cpb.2009.0068

Ministère de la Justice. (2017). *Cyberintimidation et distribution non consensuelle d'images intimes.* https://www.justice.gc.ca/fra/pr-rp/autre-other/cdncii-cndii/p6.html

Ministère de la Sécurité publique. (2021). *Statistique de la criminalité au Québec : principales tendances 2016*. Direction de la prévention et de l'organisation policière. https://www.securitepublique.gouv.qc.ca/fileadmin/Documents/police/statistiques/criminalite/2016/stats_criminalite_2016_2.pdf

Mumporeze, N., Han-Jin, E. et Nduhura, D. (2021). Let's Spend a Night Together; I Will Increase Your Salary: An Analysis of Sextortion Phenomenon in Rwandan Society. *Journal of sexual aggression*, *27*(1), 120-137.

Murr, H. S. (2006). The Continuing Expansive Pressure to Hold Employers Strictly Liable for Supervisory Sexual Extortion: An Alternative Approach Based on Reasonableness. *GGU Law Digital Commo*n. *39*, 529-636.

Navarro, J. N. et Jasinski, J. L. (2013). Why Girls? Using Routine Activities Theory to Cyberbullying Experiences Between Girls and Boys. *Women & Criminal Justice*, 23(4), 286-303. https://doi.org/10.1080/08974454.2013.784225

Nelson, B. W., Pettitt, A., Flannery, J. E. et Allen N .B. (2020) Rapid Assessment of Psychological and Epidemiological Correlates of COVID-19 Concern, Financial Strain, and Health-related Behavior Change in a Large Online Sample. *PLoS ONE 15*(11): e0241990. https://doi.org/10.1371/journal.pone.0241990

O'Malley, R. L. et Holt, K. M. (2020). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of interpersonal violence*, *37*(1-2), 258-283.

O'Malley, R. L. et Holt, K. M. (2022). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of Interpersonal Violence*, *37*(1-2), 258-283. https://doi.org/10.1177/0886260520909186

Paat, Y.-F. et Markham, C. (2021). Digital Crime, Trauma, and Abuse: Internet Safety andCyber Risks for Adolescents and Emerging Adults in the 21st Century. *Social Work in Mental Health*, *19*(1), 18-40. https://doi.org/10.1080/15332985.2020.1845281

Palmer, T. (2015). Digital Dangers: The Impact of Technology on the Sexual Abuse and Exploitation of Children and Young People. *Barnardo's, available online at http://www. barnardos. org. uk/onlineshop/pdf/digital_dangers_report. pdf*

Patchin, J. W. et Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of US Youth. *Sexual Abuse,* 32(1), 30-54.

Powell, A. et Henry, N. (2017). *Sexual Violence in a Digital Age*. Basingstoke: Palgrave Macmillan.

Powell, A., Henry, N., Flynn, A. et Scott, A. J. (2019). Image-based Sexual Abuse: The Extent, Nature, and Predictors of Perpetration in a Community Sample of Australian Residents. *Computers in Human Behavior*, *92*, 393-402. https://doi.org/10.1016/j.chb.2018.11.009

Reyns, B. W., Henson, B. et Fisher, B. S. (2011). Applying Cyber Lifestyle-routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behaviour, 38*, 1149-1169. DOI: 10.1177/0093854811421448

Reyns, B. W., Henson, B. et Fisher, E. S. (2016). Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as it Applies to Online Forms of Victimization. *Journal of Contemporary Justice, 32*(2), 148-168. https://doi.org/10.1177/1043986215621378

Ringrose, J., Regehr, K. et Whitehead, S. (2021). 'Wanna Trade?': Cisheteronormative Homosocial Masculinity and the Normalization of Abuse in Youth Digital Sexual Image Exchange. *Journal of Gender Studies*, *31*(2), 243-261.

Sales, N. J. (2016). *American Girls: Social Media and the Secret Lives of Teenagers*. Knopf Doubleday Publishing Group.

Salter, M. et Crofts, T. (2015). Responding to Revenge Porn: Challenging Online Legal Impunity. Dans L. Comella et S. Tarrant (dir.), *New Views on Pornography: Sexuality, Politics and the Law* (233–256). Westport : Praeger Publisher.

Saint-Louboue, L. (2020). La face cachée des réseaux sociaux : cyberharcèlement chez les mineurs. *Annales médico-psychologiques, revue psychiatrique, 178*(4), 419-422. https://doi.org/10.1016/j.amp.2020.02.010

Sedgwick, E. K. (1985). Between Men: English Literature and Male Homosocial Desire. Columbia University Press.

Statistiques Canada (2020) Statistiques sur les crimes declarés par la police au Canada, *Statistiques Canadaé* Tiré de : https://www150.statcan.gc.ca/n1/pub/85-002-x/2021001/article/00013-fra.htm

Transparency International (23 septembre 2019) Global Corruption Barometer 2019- Women & Corruption in Latin America and The Carribbean. Tiré de: https://www.transparency.org/en/publications/global-corruption-barometer-lac-2019-women-corruption

Uhl, C. A., Rhyner, K. J., Terrance, C. A. et Lugo, N.R. (2018). An Examination of Nonconsensual Pornography Websites. *Feminism & Psychology*, 28(1), 50-68. https://doi-org/10.1177/0959353517720225

Vakhitova, Z. I., Alston-Know, C. L., Reynald, D. M., Townsley, M. K. et Webster, J. L. (2019). Lifestyles and Routine Activities: Do They Enable Different Types of Cyberabuse?. *Computers in Human Behavior, 101*, 225-237. https://doi.org/10.1016/j.chb.2019.07.012

Vasiu, I. et Vasiu, L. (2020). Forms and Consequences of the Cyber Threats and Extortion Phenomenon. *European Journal of Sustainable Development*, *9*(4), 295-2950 https://doi.org/10.14207/ejsd.2020.v9n4p295

Wittes, B., Poplin, C., Jurecic, Q. et Spera, C. (2016, 11 mars). Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault. *Brookings*. https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/

Wolak, J et Finkhelor, D. (2016). *Sextortion: Findings from a Survey of 1,631 Victims*. https://calio.dspacedirect.org/handle/11212/3037

Wolak, J., Finkelhor, D., Walsh, W. et Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, *62*(1), 72-79.

Young, S. M., Pruett, J. A. et Colvin, M. L. (2018). Comparing Help-seeking Behavior of Male and Female Survivors of Sexual Assault: A Content Analysis of a Hotline. *Sexual Abuse*, *30*(4), 454-474.

ANNEXE 1 : Chronique sur la sextorsion en contexte militaire

Écrit par Alexis Rapin, chercheur en résidence à l'Observatoire sur les conflits multidimensionnels

Ce texte est d'abord paru le 26 avril 2022 en tant que Chronique des nouvelles conflictualités écrite dans le cadre du partenariat entre Les 3 sex* et la Chaire de recherche Raoul-Dandurand en études stratégiques et diplomatiques.

Personnel militaire : de la sextorsion au « sexpionnage »?

Alors que de plus en plus de membres des forces armées à travers le monde recourent aux plateformes de rencontre pour pallier la solitude de la vie en caserne, les institutions militaires s'inquiètent : les romances en ligne peuvent représenter un moyen de soutirer de l'information à valeur stratégique, qu'elles soient vraies ou fausses.

La géopolitique s'arrête-t-elle à la sphère intime? Rien n'est moins sûr. À travers le monde, de plus en plus de forces armées s'inquiètent du fléau grandissant de la sextorsion, soit l'usage d'images ou de vidéos à caractère sexuel comme moyen de pression contre des individus. Entre autres craintes : que des puissances adverses en viennent à soutirer des informations sensibles à du personnel militaire par l'entremise de contenu intime, par exemple obtenu via de fausses romances sur Internet.

Si le scénario peut faire sourire, les Forces armées américaines, elles, prennent le problème très au sérieux : en 2019, le département de la Défense et l'Armée américainediffusaient déjà à leur personnel des avertissements officiels à ce sujet. Bien que la préoccupation majeure reste pour l'heure le bien-être des victimes elles-mêmes, de plus en plus de voix font remarquer que le phénomène pourrait à l'avenir soulever des enjeux plus stratégiques : les actes de sextorsion, jusqu'ici utilisés par des criminels notamment dans le but de s'enrichir, pourraient tout aussi bien servir à des acteurs politiques pour obtenir des informations à valeur stratégique. Tinder, Bumble,Hinge et autres plateformes de ce monde seraient-ils en passe de devenir les nouveaux terrains de chasse du renseignement militaire?

Groupes bien organisés

À l'origine du problème, on trouve un phénomène à bien des égards facile à appréhender : les forces armées comptent dans leurs rangs beaucoup de jeunes individus déployés loin de chez eux et de leurs cercles sociaux, et bien souvent aux prises avec la solitude de la vie en caserne. En quête de romance (ou plus si affinités), de nombreux militaires recourent à des sites ou des applications de rencontre, sur lesquels tout le monde n'est pas forcément la personne prétendue. On imagine aisément la suite : discussions aguichantes, propositions d'échanges de photos intimes et potentiellement appels vidéo, à travers lesquels les victimes en viennent à s'exposer. Les personnes commettant des fraudes, elles, utilisent le plus souvent des photos volées ou des vidéos pornographiques préenregistrées pour amadouer leurs allocutaires. Et voilà le piège refermé.

De quelques cas isolés à partir de 2012, le phénomène n'a pas tardé à faire les manchettes aux États-Unis : en novembre 2018, le Pentagone annonçait le démantèlement d'un réseau criminel ayant sextorqué plus d'un demi-million de dollars américains à quelque 440 membres des forces armées. Derrière de charmants faux profils sur les réseaux sociaux se cachait en fait… un groupe de détenus sévissant discrètement depuis une prison de Caroline du Sud. D'autres

cas traités par les unités d'investigation criminelle des Forces armées américaines mettaient en cause des groupes basés aux Philippines ou en Côte d'Ivoire, présentant parfois un haut degré d'organisation. L'un des réseaux philippins comptait par exemple près d'une cinquantaine de membres travaillant dans un bureau centralisé, et fonctionnait sur la base d'une grille salariale bien établie, prévoyant des bonus pour les individus ayant extorqué les plus grosses sommes.

Scandales sur demande

De quoi donner quelques sueurs froides aux agences de contre-espionnage. De telles officines ne sont en effet pas sans rappeler les usines à trolls qui, aux quatre coins du monde, sont de plus en plus mandatées par des acteurs malveillants pour mener des campagnes de désinformation à l'étranger. Profitant de systèmes judiciaires locaux souvent dysfonctionnels et offrant un potentiel de déni aux acteurs qui les emploient, ces entités se présentent de plus en plus comme des sous-traitants d'opérations clandestines orchestrées par des États. On peut ainsi craindre que les groupes organisés pratiquant la sextorsion n'en viennent à s'inspirer de ce modèle d'affaires, en louant par exemple leurs services à des puissances étrangères pour piéger et faire chanter des individus en position de pouvoir dans des pays rivaux.

De premiers cas de scandales à caractère intime s'approchent de tels schémas. En 2018 en Ukraine, deux sulfureux consultants en relations publiques ont été arrêtés pour avoir orchestré une fausse relation Tinder impliquant un haut placé de la police nationale. Empruntant le compte Tinder d'une jeune étudiante, les malfaiteurs ont créé de toute pièce une discussion en ligne dans laquelle le haut fonctionnaire semblait solliciter des faveurs sexuelles, échange par la suite fuité dans la presse ukrainienne. Alors que les consultants semblent avoir reçu une somme importante pour leurs services, l'identité des mandataires du coup monté reste inconnue, mais divers observateurs furent prompts à suggérer une possible implication de la Russie.

Des *kompromats* 2.0

Si le « scandale Tinder » en Ukraine n'était que supercherie, d'autres tentatives d'instrumentalisation stratégique de relations intimes en ligne s'accumulent. En 2018, par exemple, l'Armée israélienne révélait que le Hamas avait mis sur pied plusieurs applications de rencontre frauduleuses, truffées de faux profils de jeunes femmes, pour tenter de duper des soldats de Tsahal et de leur soutirer des renseignements. En 2020, l'Armée indienne interdisait à ses soldats l'usage de près de 90 applications de rencontre, affirmant que le renseignement pakistanais les utilisait à des fins d'espionnage.

Dans certains cas, ces fausses romances servent seulement à faciliter des piratages informatiques classiques, les échanges de mots doux endormant la vigilance des utilisateurs et utilisatrices, les poussant ainsi à cliquer sur des liens infectés par exemple. Parfois, c'est davantage le chantage émotionnel qui semble exploité : l'amant.e virtuel.le force subtilement la cible à révéler des informations confidentielles à grand renfort de jeu sentimental. Dans d'autres cas, enfin, ces opérations semblent carrément avoir vocation à piéger la victime et récolter des « *kompromats* 2.0 », des contenus embarrassants, bien souvent à caractère sexuel, susceptibles de la faire chanter. L'information ainsi obtenue peut prendre de nombreuses formes : emplacements et rotations d'unités, détails sensibles sur du matériel ou des infrastructures militaires, structure et organisation des chaînes de commandement, etc.

Au Canada, un avertissement

Si les institutions militaires se montrent actuellement parmi les plus préoccupées face au péril du « sexpionnage », il est clair que la problématique ne se cantonne pas aux seules forces armées : diplomates, haut fonctionnaires et autres figures en position de pouvoir constituent aussi d'évidentes cibles potentielles à qui soutirer de l'information sensible par l'entremise de fausses romances en ligne. Début 2022, dans son allocution annuelle, le directeur du renseignement intérieur australien avertissait publiquement ses concitoyen.ne.s des risques géopolitiques posés par les plateformes de rencontre instrumentalisées par des services d'espionnage étrangers.

Le Canada, quant à lui, a même déjà senti le vent du boulet : en novembre 2018, le député conservateur et ex-ministre Tony Clement s'est retrouvé au cœur d'une affaire de sextorsion menée depuis l'étranger. Croyant entretenir une relation en ligne avec une femme se disant «en quête d'amour », le politicien avait envoyé des photos sexuellement explicites à celle-ci, sans se douter qu'il était en fait piégé par les membres d'un réseau d'escroquerie basé en Côte d'Ivoire. Tony Clement s'était ensuite fait réclamer le versement de 75 000 dollars, faute de quoi les photos seraient publiées. Le député fut poussé à la démission à la suite du scandale, et deux des malfaiteurs furent plus tard appréhendés par les autorités ivoiriennes.

L'affaire livra toutefois un aperçu, voire un avertissement, quant aux potentielles retombées géopolitiques de la sextorsion : au moment des faits, Tony Clement était en effet appelé à siéger prochainement sur le Comité des parlementaires sur la sécurité nationale et le renseignement, alors fraîchement créé par le gouvernement Trudeau. Il aurait eu, dans le cadre de cette fonction, accès à des informations classifiées et extrêmement sensibles, touchant par exemple aux activités du Service canadien de renseignement de sécurité, du Centre pour la sécurité des télécommunications ou encore du ministère de la Défense. Certain.e.s firent ainsi remarquer que l'affaire, si elle n'avait pas été révélée à temps, aurait fourni un potentiel outil de chantage de premier choix à des puissances étrangères en quête de secrets d'État.

LEXIQUE

Agentivité : Terme utilisé pour décrire la faculté d'un agent à exercer un pouvoir ou une influence sur les choses, les évènements, les êtres ou le monde.

Authentification à deux facteurs : En plus de demander simplement un mot de passe, l'authentification à deux facteurs demande une deuxième vérification, par exemple l'envoi d'un code temporaire par courrier électronique ou par SMS dont la saisie est nécessaire pour se connecter. Elle est utilisé pour réduire la probabilité qu'un compte soit piraté.

Capping : Technique qui consiste à enregistrer des séquences vidéo ou des captures d'écran sans le consentement de la personne exposée. En marketing, le capping réfère plutôt à une technique limitant le nombre d'affichage d'une publicité en ligne.

Catcalling : Harcèlement verbal sous forme de commentaires chargés sexuellement, d'avances ou de compliments sexuels non sollicités, généralement faits en passant dans un lieu public.

Catfishing : Acte de se présenter frauduleusement en ligne. Il peut s'agir de se faire passer pour une personne fictive, un autre individu ou une version antérieure de soi-même (par exemple, nettement plus jeune ou plus séduisante). Technique souvent utilisée pour s'engager de manière trompeuse dans une relation amoureuse avec la victime à des fins de gain financier, pour la manipuler, l'humilier, la faire souffrir ou pour réaliser ses souhaits.

Culture du viol : Système social dans lequel les croyances, les attitudes et les valeurs concernant la sexualité et le genre banalisent et normalisent la violence sexuelle, y compris le viol. La culture du viol est un terme de plus en plus utilisé afin de mettre en exergue des comportements sociaux qui excusent et légitiment les violences à caractère sexuel.

Cybermobs : Groupe de personnes qui se liguent pour mener une campagne en ligne contre un individu qui a commis une transgression sociale réelle ou perçue. Ces *mobs* s'intensifient souvent en harcèlement, qui peut inclure des menaces et des discours de haine. Elles accablent effectivement la victime en raison de l'ampleur, de la persistance et de la gravité des attaques.

Deepfake : Un *deepfakes* est un vidéos hyperréaliste réalisé par le biais de techniques d'intelligence artificielle, et dépeignant des personnes disant et faisant des choses qui n'ont jamais eu lieu. Des techniques de *deepfakes* sont ainsi utilisées à des fins malveillantes, par exemple pour créer des vidéos pornographiques où figurent des personnalités célèbres.

Digital fingerprinting : Algorithme qui crée une signature unique d'un fichier (voir *Hashing*) qui peut ensuite être comparée à d'autres fichiers dans la base de données. Il est utilisé pour détecter, bloquer et supprimer les fichiers (tels que les images ou les vidéos) qui correspondent à la signature.

Doxing : Fait de publier en ligne les informations personnelles d'une personne dans le but d'inciter les foules au harcèlement et/ou à la violence envers l'individu en question.

Downblousing : Acte de filmer ou de photographier dans la chemise, la robe ou tout autre vêtement d'une femme sans son consentement dans le but de capturer ses seins ou son décolleté.

E-whoring : Technique d'ingénierie sociale dans laquelle l'auteur du crime crée un profil frauduleux en se faisant passer pour une fille séduisante et en incitant les gens à payer pour du

contenu explicite (qui a généralement été volé ou divulgué). Les auteurs forment des réseaux pour échanger et vendre des ballots de contenu ainsi que pour partager des informations et des techniques afin de maximiser les profits.

Fraude romantique : Création d'un faux profil dans le but de se faire passer pour une autre personne afin de gagner l'affection et la confiance de sa victime pour tranquillement sexualiser la relation, la mener à partager du contenu explicite pour ensuite la soumettre à nos demandes.

Hameçonnage (phishing) : Technique d'ingénierie sociale qui consiste à une attaque qui tente de voler des données ou de l'argent en envoyant un message frauduleux se faisant passer pour un courriel ou un site Web légitime qui incite la personne à révéler des informations personnelles et/ou confidentielles, ou à télécharger un logiciel malveillant (voir *Maliciel*).

Hashing : Signature unique donnée à un fichier. Il est utilisé pour détecter, bloquer et supprimer les fichiers (tels que les images ou les vidéos) qui correspondent à la signature.

Maliciels : L'utilisation de maliciels (logiciels malicieux) est une tactique d'ingénierie sociale qui vise à endommager ou perturber un ordinateur, un serveur ou un réseau, prendre le contrôle de ses opérations, obtenir et divulguer des informations privées, etc.

Partage non consensuel d'image intime : Fait de partager des images intimes sans le consentement de la ou des personnes représentées dans ces images. Le partage de ces images n'est pas nécessairement facilité par la technologie.

Pornographie mainstream : Pornographie à succès commercial produite par de grands studios dans laquelle la domination masculine, le plaisir axé sur l'homme, le sexe hétérosexuel avec pénétration, l'humiliation/dégradation de la femme sont mis de l'avant.

Revenge porn : Familièrement compris comme l'acte de vengeance d'un.e ex-amant.e méprisé.e qui partage du contenu sexuellement explicite sans le consentement de son ancien.ne partenaire.

Réseaux privés virtuels (VPN) : Étend un réseau Internet privé à un réseau Internet public en utilisant le cryptage. Utilisé pour masquer les données d'une personne telles que son adresse IP, sa localisation et son historique de navigation.

Serveurs proxy : Système informatique qui sert d'intermédiaire entre l'internaute et le serveur fournissant une ressource à laquelle l'internaute tente d'accéder. Utilisé pour protéger l'internaute contre le piratage.

Scammer : Personne qui perpétue une escroquerie, un stratagème malhonnête ou une fraude, souvent dans un but lucratif.

Sextage : Création, envoi ou réception de messages textes à caractère sexuel. Les sextos peuvent inclure, ou non, du contenu vidéo, photographique ou audio. La plupart du temps, le sextage prend la forme de contenu imagé représentant de la nudité partielle, totale ou des actes sexuels.

Sexters : Personne qui envoie des communications sexuellement explicites par le biais d'un chat, d'un texto électronique ou d'un autre service de messagerie numérique.

Sextos : Communication sexuellement explicite envoyée par chat, courrier électronique ou autre service de messagerie numérique.

Technologies de l'information et de la communication (TIC) : Toute forme de technologie de l'information permettant d'accéder aux communications, de les transmettre, de les stocker, de les comprendre et de les manipuler, y compris, mais sans s'y limiter, la radio, la télévision, les téléphones portables, les ordinateurs.

Upskirting : Filmer ou photographier sans consentement sous les jupes avec l'intention de capturer des images/vidéos de sous-vêtements ou de parties génitales.

Vidéovoyeurisme : Accès illégal aux caméras sur l'ordinateur d'une personne afin de l'observer à son insu.

Violence à caractère sexuelle facilité par la technologie (VCSFT) : Fait d'instrumentaliser la technologie pour exercer une violence sexuelle dans le monde virtuel ou physique, y compris le cyberharcèlement sexuel, la violence sexuelle basée sur l'image, l'agression et la coercition sexuelles, et le harcèlement sexuel basé sur le genre et la sexualité.

Violence à caractère sexuel basée sur l'image (VCSBI) : Continuum proposé par McGlynn et Rackley (2017) qui se situe comme une forme d'abus dans un continuum encore plus large de violence sexuelle proposé par Kelly (1988). Ce concept met en évidence des points communs sous-jacents (abus et harcèlement sexués et sexualisés) reliant ce qui pourrait autrement être interprété comme des phénomènes distincts : la création non consensuelle d'images intimes, la distribution non consensuelle d'images intimes (PNCII), la menace de partage d'images intimes, etc.