Les traces numériques laissées par les cyberdélinquants sexuels : identités virtuelles, mensonges et protection de l'anonymat

Par **Sarah PAQUETTE*** et **Francis FORTIN****

RÉSUMÉ

En regard de ses avantages perçus, nombre d'individus utilisent l'internet, les technologies numériques et les réseaux sociaux pour exploiter des jeunes à des fins sexuelles. Considérant la présence policière accrue en ligne, notre hypothèse est que les cyberdélinquants sexuels, soucieux des risques associés à leurs activités illégales, tendent à adopter diverses stratégies afin de masquer les traces numériques qu'ils laissent, dans l'espoir de préserver leur anonymat. L'objectif de cette étude est de dresser le portrait des identités virtuelles et activités de subterfuges entreprissent par 161 cyberdélinquants sexuels, avec un intérêt particulier sur les tendances contemporaines. Utilisant les données du projet de recherche PRESEL, cette étude examine les caractéristiques des identités virtuelles et des plateformes de clavardage (discussion en ligne) utilisées par les hommes qui sollicitent les jeunes en ligne à des fins sexuelles, ainsi que des outils technologiques d'acquisition du matériel des hommes qui consomment de la pornographie juvénile. Des analyses corrélationnelles ont été réalisées afin d'examiner les liens unissant la propension à utiliser les techniques numériques de préservation de l'anonymat et les paramètres du crime. Les résultats montrent que même si les stratégies de protection de l'identité sont plus fréquemment utilisées par les cyberdélinquants que les stratégies de protection des systèmes informatiques, un plus grand nombre n'utilise aucune stratégie. Par ailleurs, les résultats suggèrent que le niveau d'engagement dans la criminalité et la contemporanéité des cybercrimes influencent la propension à la préservation de l'anonymat en ligne, alors que l'âge n'a aucun impact. Les implications pour la recherche et la pratique des enquêtes criminelles en ligne sont discutées.

Mots clés: sollicitation sexuelle d'enfant, pornographie juvénile, trace numérique, identité virtuelle, protection de l'identité.

ABSTRACT

In view of its perceived advantages, many people use the internet, digital technologies and social networks to sexually exploit minors. In light of the increased police presence on the internet, our hypothesis is that online sexual offenders concerned about the risks associated with their illegal activities tend to adopt various strategies to hide the digital traces they leave, in the hope of preserving their anonymity. The objective of this study

* Ecole de travail social et criminologie, Université Laval ; Division provinciale de la coordination des délinquants sexuels, Sûreté du Québec.

** Ecole de criminologie, Université de Montréal.

was to draw a portrait of the virtual identities and subterfuge activities undertaken by 161 online sexual offenders, with a particular focus on contemporary trends. Using data from the PRESEL research project, this study examines the characteristics of virtual identities and chat platforms used by men who sexually solicit young people online, as well as the tools used to acquire the material of men who use child pornography. Correlational analyses were conducted to examine the links between the propensity to use digital anonymity preservation techniques and crime parameters. Results showed that even if identity protection strategies were more frequently used by online offenders than computer system protection strategies, more offenders did not use any strategy. Furthermore, results suggest that the engagement in criminality and the contemporaneity of cybercrimes influences the propensity of preserving anonymity online, while age has no such impact. The implications for research and practice of online crime investigation are discussed.

Keywords: child sexual solicitation, child pornography, digital trace, virtual identity, identity protection.

Introduction

L'émergence de l'internet, le développement des technologies numériques et la création des réseaux sociaux virtuels ont offert de nouveaux lieux, perçus par plusieurs comme offrant un certain anonymat (Cooper, 1998, 2002), pour y commettre des comportements illégaux, y compris de nature sexuelle envers les enfants. Le nombre de dénonciations reçues par les autorités policières pour des infractions relatives à la pornographie juvénile ou la sollicitation sexuelle de personnes mineures est d'ailleurs en augmentation chaque année. Au Canada, entre 2008 et 2015, le nombre de signalements pour ce type d'infraction a augmenté de 376 %, atteignant 37 352 en 2015 (Cyberaide, 2016). Aux États-Unis en 2010, plus de 20 millions d'adresses de protocole internet (IP) étaient associées au partage de pédopornographie (US Department of Justice, 2010). Considérant l'ampleur du phénomène et les conséquences négatives qui y sont associées, plusieurs chercheurs ont examiné les caractéristiques des cyberdélinquants sexuels (p.ex., Babchishin et al., 2015 ; Seto et al., 2012), n'abordant que partiellement la question de l'anonymat. Or, les identités virtuelles que revêtent les cyberdélinquants sont parfois transformées dans le but d'attirer des victimes potentielles, mais également pour éviter la détection policière (p.ex., Briggs et al., 2011 ; Dowdell et al., 2011 ; Wolak et al., 2004). L'utilisation de l'internet laisse toutefois des traces numériques pouvant rendre les cyberdélinquants sexuels à risque de détection policière (Wolak et al., 2011). Cette étude porte sur les identités virtuelles utilisées par les cyberdélinquants sexuels ainsi que sur les stratégies de subterfuges qu'ils adoptent à l'occasion de leurs activités sexuelles en ligne pour se présenter sous un meilleur jour ou pour préserver leur anonymat face à une possible détection policière.

Les profils des cyberdélinquants sexuels

Les cyberdélinquants sexuels sont en grande majorité des hommes (environ 99 % ; Seto, 2013), bien que des femmes aient été identifiées dans la littérature scientifique de manière anecdotique (p.ex., Eke et al., 2011 ; Prat et al., 2014). Plusieurs caractéristiques distinguent les hommes qui commettent leurs délits sexuels en ligne de ceux qui les commettent hors ligne, notamment leurs capacités cognitives et niveaux d'éducation plus élevés, leur sexualité plus problématique et leur meilleure autorégulation (Babshichin et al., 2011, 2015). Ces caractéristiques réunies laissent supposer que ces délinquants, à tout le moins certains, seraient disposés à déployer des stratégies astucieuses ou sophistiquées pour actualiser leurs intérêts et fantaisies atypiques en utilisant l'internet. Cette hypothèse serait d'ailleurs cohérente avec les données indiquant qu'une faible portion (12 %) des cyberdélinquants ont été formellement accusés de crimes avec contact envers des enfants, alors que bien plus (55 %) ont admis avoir commis de tels crimes sans toutefois avoir fait l'objet de sanctions judiciaires (Seto et al., 2011). Par ailleurs, le niveau de technicité informatique, reflété par l'utilisation de méthodes de chiffrement ou de protection de l'identité, distinguerait les cyberdélinquants sexuels prudents des imprudents (Krone, 2005 ; Fortin et al., 2017 ; Fortin, 2006). Les cyberdélinquants avec de meilleures connaissances techniques seraient d'ailleurs plus sensibles aux risques inhérents associés à leurs comportements illégaux en ligne (Eneman, 2009 ; Balfe et al., 2015).

Si la plupart des consommateurs de matériel pédopornographique s'engagent dans leurs activités virtuelles de manière solitaire (Fortin et al., 2017), ne laissant ainsi que peu de traces numériques sur des profils virtuels, les hommes qui communiquent avec des personnes mineures à des fins sexuelles sont, pour leur part, de plus en plus présents sur les réseaux sociaux et les plateformes de clavardage (Balfe et al., 2015 ; Mitchell et al., 2010). Une variété de plateformes et d'applications est dorénavant offerte aux internautes pour clavarder, certaines offrant même la possibilité d'y créer des profils détaillés (p.ex., Facebook), alors que d'autres ne requièrent l'inscription que d'un minimum d'informations personnelles (p.ex., Instagram). Il demeure toutefois à la discrétion des utilisateurs d'y inscrire des informations véridiques ou mensongères.

Le mensonge est une composante importante à considérer pour la compréhension du modus operandi des cyberdélinquants. Dans une étude menée auprès d'agences policières aux États-Unis, une proportion considérable d'hommes condamnés pour des crimes sexuels hors ligne à la suite de sollicitation de personnes mineures en ligne (n = 129) avaient menti à leurs victimes à propos de leur identité : 25 % ont affirmé être plus jeunes qu'ils ne l'étaient en réalité et 26 % ont menti sur leur apparence physique ou sur d'autres aspects de leur identité (Wolak et al., 2004). Dans un autre sondage, 71 % des hommes qui ont sollicité à des fins sexuelles des personnes mineures et qui ne possédaient aucun antécédent de crime

sexuel hors ligne (*n* = 113) avaient fourni des informations mensongères à leurs victimes quant à leur identité : 83 % ont systématiquement menti à propos de leur nom ou leur âge, alors que d'autres 17 % l'ont fait de manière occasionnelle (Dowdell et al., 2011). La tendance à mentir dans cette étude diminuait toutefois auprès des hommes ayant un historique de contact sexuel hors ligne envers des mineurs, alors que seuls 48 % (*n* = 236) avaient menti à leurs victimes. Dans une étude sur la sextortion en ligne, 89 % des hommes qui ciblaient spécifiquement des jeunes avaient recours à des stratégies de manipulation, notamment en mentant sur leur âge (en se rajeunissant) et sur leur genre (en prétendant être une jeune femme) afin de gagner la confiance de leurs victimes et les inciter à obtempérer face à leurs demandes sexuelles (O'Malley et Holt, 2020). La variabilité des taux de divulgation de fausses informations personnelles dans ces études est possiblement attribuable aux finalités visées par les cyberdélinquants qui clavardent avec des jeunes. Il semble en effet que les cyberdélinquants désireux d'obtenir des rencontres hors ligne avec leurs victimes seraient moins enclins à mentir que ceux qui restreignent leurs infractions au Web. Plus d'études seraient toutefois nécessaires afin de tester cette hypothèse de manière empirique.

L'utilisation des technologies par les hommes qui clavardent avec des jeunes à des fins sexuelles

Différentes motivations sous-tendent l'exploitation sexuelle des jeunes. Parmi celles-ci se trouve l'intérêt préférentiel pour les enfants, mais également l'intérêt non préférentiel pour les enfants et la saisie d'opportunités (Babchishin et al., 2015). Pour les hommes qui cherchent spécifiquement à entrer en communication avec des jeunes, le choix des plateformes de clavardage s'oriente vers des endroits où la prévalence de jeune est importante. Ils auront notamment tendance à privilégier Instagram ou Facebook, lesquelles figurent parmi les plus utilisées par les adolescents en 2020 (Statistica, 2021). Le choix des hommes présentant un intérêt non préférentiel pour les jeunes sera également guidé par leur motivation et les opportunités. Les données obtenues du sondage de Dowdell et ses collaborateurs (2011) montrent que plus de la moitié (57 %) des cyberdélinquants sollicitaient des mineurs présents dans des chambres de discussion « d'âge approprié », c'est-à-dire des forums virtuels dédiés aux adultes. En l'absence d'opportunité pour s'engager dans des activités sexuelles avec des adultes, certains se tournent vers les adolescents, par facilité, mais également parce que les jeunes sont perçus par les cyberdélinquants comme étant moins enclins à juger ou rejeter que les adultes (O'Malley et Holt, 2020 ; Paquette et Cortoni, 2020).

Dans une revue systématique de la littérature portant sur les technologies numériques et stratégies de préservation de l'anonymat utilisées par les cyberdélinquants sexuels, des chercheurs ont trouvé que plusieurs utilisaient

des plateformes qui ont pourtant été largement délaissées par le grand public, notamment les groupes de discussion et les salons de clavardage (Balfe et al., 2015). Concernant la reconnaissance des risques inhérents associés à l'utilisation de l'internet pour la commission d'infractions sexuelles, ces chercheurs suggèrent qu'il existerait un continuum sur lequel se situerait, à une extrémité, les cyberdélinquants peu soucieux des risques (voir Beech et al., 2008 ; Briggs et al., 2011 ; Glasgow, 2010), et à l'autre, ceux particulièrement sensibles (voir D'Ovidio et al., 2009 ; Eneman, 2009 ; Holt et al., 2010 ; Ray et al., 2010 ; Sheehan et Sullivan, 2010). Les moins soucieux révèleraient plus d'informations personnelles, notamment à propos de leur véritable nom, âge et occupation (Briggs et al., 2011). À l'opposé, les plus sensibles utiliseraient, quant à eux, différentes stratégies afin de protéger leur identité comme l'utilisation d'ordinateurs ou d'appareils intelligents spécifiquement dédiés à leurs activités illégales et non accessibles à leur entourage, l'utilisation de pseudonymes, et la communication sur des plateformes ou espaces privés (p.ex., courriel, Facebook Messenger, messagerie textuelle) (Balfe et al., 2015 ; Graham, 2000 ; Holt et al., 2010 ; Kierkergaard, 2011 ; Webster, 2012).

L'utilisation des technologies par les consommateurs de pornographie juvénile

Diverses méthodes d'acquisition de matériel pédopornographique ont été identifiées par les chercheurs, certaines laissant des traces numériques permettant facilement l'identification des auteurs de cybercrimes, d'autres laissant des traces numériques plus difficilement reliées à l'identité véritable des suspects. Parmi ces méthodes se trouve l'utilisation de logiciels de partage pair à pair (poste-à-poste) dont la fonction principale est le partage de fichiers numériques, notamment la musique, les photos et les vidéos, par l'entremise d'autres internautes dont le système informatique agit en guise de serveur (Fortin et al., 2017 ; Wortley et Smallbone, 2006). Les requêtes effectuées via ces logiciels ne font pas spécifiquement l'objet d'une protection puisque l'adresse IP véritable des internautes est associée aux échanges effectués entre les pairs. Cependant, ces adresses peuvent être découvertes et indexées grâce à des outils de détection automatique de matériel illégal, tel que le *Child Protection System* (CPS), utilisé par les agences d'application de la loi pour identifier les distributeurs de pornographie juvénile (Liberatore et al., 2010 ; Solon, 2020 ; Wolak et al., 2011). Même si la technologie est considérée très vieille, les logiciels poste-à-poste étaient encore, à venir jusqu'en 2011, l'une des sources d'acquisition de pédopornographie les plus populaires (Kierkergaard, 2011 ; Wolak et al., 2014). Une décennie plus tard, il est toutefois incertain si cette technologie a toujours primauté parmi les méthodes d'acquisition du matériel des cyberdélinquants sexuels. Des données rapportées par les autorités policières américaines montrent que sur une période d'une année, plus de 870 millions de fichiers de pornographie juvénile ont été partagés via

les logiciels poste-à-poste à partir de 775 941 ordinateurs situés dans plus de 100 pays à travers le monde (Wolak et al., 2014).

L'acquisition de matériel d'abus sexuel d'enfant peut aussi s'obtenir dans le cadre d'infractions adjacentes. Ainsi, un grand nombre des cyberdélinquants font l'acquisition d'images de nature sexuelle de leurs victimes adolescentes dans le cadre de leur communication en ligne : 60 % l'ont fait selon une étude nationale menée par le *National Center for Missing & Exploited Children* (NCMEC, 2017). De plus, pour 55 % des auteurs de sextortion envers les jeunes de l'échantillon de O'Malley et Holt (2020), les communications en ligne s'inscrivaient plus largement dans leurs activités d'acquisition de pornographie juvénile.

La présence en ligne des cyberdélinquants offre aussi maintes occasions pour se familiariser aux pratiques efficientes dans le domaine. Certains utilisent les plateformes virtuelles pour clavarder avec des internautes pour obtenir des conseils sur la manière de procéder pour obtenir du matériel pédopornographique, notamment les mots-clés les plus efficaces et logiciels de prédilection, mais également sur les stratégies à adopter pour éviter la détection policière (voir Fortin et al., 2017). Parmi ces stratégies, notons l'intérêt récent pour le Dark Web sur lequel l'ensemble des activités virtuelles sont chiffrées (Owen et Savage, 2015). Tor, un navigateur du Dark Web, a été d'ailleurs conçu pour les internautes désireux de préserver l'anonymat en ligne et est utilisé par nombre de cyberdélinquants (Gehl, 2016 ; Graham et Pitman, 2018). Même si le nombre de cyberdélinquants sexuels présents sur le Dark Web est difficilement quantifiable, on estime que 2 % des contenus disponibles sont consacrés à la pédopornographique et que la navigation des pédophiles constituerait plus de 80 % du trafic global du Dark Web (Haasz, 2016).

Au-delà de l'utilisation du Dark Web qui nécessite des connaissances spécifiques en raison du fait qu'il n'est pas accessible par les moteurs de recherche traditionnels et qui parfois rebute par sa lenteur (Gehl, 2016 ; Graham et Pitman, 2018 ; Haasz, 2016), d'autres technologies sont à la disposition des cyberdélinquants pour préserver l'anonymat à l'occasion de leurs activités d'acquisition de pornographie juvénile. À cet effet, Balfe et ses collaborateurs (2015) notent entre autres l'utilisation du chiffrement et de serveurs proxy. Ces technologies ne seraient toutefois que rarement utilisées, comme indiqué par la faible portion (3 %) de consommateurs de pornographie juvénile détectés (n = 604) dans l'étude de Wolak et ses collaborateurs (2011) qui en avait fait l'usage.

La présente étude

Avec l'évolution rapide des technologies, les outils de prédilection d'hier ne sont plus forcément ceux de demain. On peut émettre l'hypothèse selon laquelle l'accessibilité des méthodes numériques de préservation

de l'anonymat aurait fait place à de nouvelles tendances quant aux pratiques virtuelles des cyberdélinquants sexuels. Une connaissance approfondie de ces pratiques est non seulement essentielle pour l'élaboration de pratiques policières proactives et efficientes, mais également pour la prévention de la victimisation sexuelle des enfants et adolescents. C'est dans ce contexte que la présente étude a été réalisée, laquelle vise deux objectifs. Le premier est de dresser le portrait des identités virtuelles et des activités de subterfuges entreprises par les cyberdélinquants sexuels, avec un intérêt particulier sur les tendances contemporaines. Le second est d'examiner les paramètres de la criminalité associés à l'utilisation de stratégies de protection de l'identité de ces cyberdélinquants.

Méthodologie

Echantillon

Les données utilisées dans le cadre de cette recherche proviennent de PRESEL, le *projet de recherche sur l'exploitation sexuelle des enfants en ligne* mené conjointement par la police provinciale du Québec (Sûreté du Québec) et des chercheurs universitaires. Ce projet vise à mieux comprendre les crimes liés à l'exploitation sexuelle de personnes mineures commis par l'entremise de l'internet. L'échantillon comprend des cas de pédopornographie ou de sollicitation sexuelle de mineurs survenus au Québec entre 2001 et 2020 pour lesquels 161 cyberdélinquants ont été reconnus coupables et pour lesquels l'ensemble des procédures judiciaires étaient terminées. À partir des dossiers de police, les informations sur les caractéristiques sociodémographiques des délinquants, leur historique criminel, leurs identités et leurs activités virtuelles en lien avec l'acquisition de pédopornographie et de sollicitation sexuelle de personnes mineures ont été recueillies et analysées.

Les caractéristiques sociodémographiques des cyberdélinquants étaient similaires aux profils des cyberdélinquants rapportés dans la littérature (Babchishin et al., 2015). Les cyberdélinquants sont tous des hommes âgés en moyenne de 39,35 ans au moment de leurs délits (É.-T. = 14,74 ; étendue = 18-81 ; n = 161). Au chapitre des antécédents criminels, ils ont en moyenne été condamnés pour 3,01 chefs de leurre d'enfants (É.-T. = 4,54 ; étendue = 0-38 ; n = 73), 1,73 chef de pornographie juvénile (É.-T. = 4,18 ; étendue = 0-34 ; n = 124), 1,45 chef lié à des crimes sexuels hors ligne (É.-T. = 2,88 ; étendue = 0-14 ; n = 64), 0,35 chef lié à des crimes violents (É.-T. = 1,36 ; étendue = 0-14 ; n = 26), 1,03 chef lié à des bris de condition (É.-T. = 2,25 ; étendue = 0-13 ; n = 49), et 1,55 chef lié aux autres catégories de crime (É.T. = 3,77, étendue = 0-19 ; n = 52).

Procédure

Dans le cadre du projet PRESEL, un manuel de codification a été élaboré par le premier auteur. Afin de s'assurer d'une validité conceptuelle et de contenu adéquat (Nunnally, 1994), la conceptualisation et l'opérationnalisation des variables ont été revues par le second auteur et un expert externe dans le domaine de la science forensique. Les variables ont été sélectionnées et définies sur la base d'un large éventail de littérature scientifique (p.ex., Cooper 1998, 2002 ; Seto, 2013) et des exemples ont été ajoutés pour guider le processus de codification. Des assistants de recherche ont été formés par le premier auteur à l'utilisation du manuel de codification. Un sous-échantillon (5 % de l'échantillon total) a été codé par deux assistants de recherche pour la fiabilité interjuges. L'accord global de la codification des variables mesurées dans PRESEL a atteint 84 %.

Ethique

Cette étude a reçu l'approbation éthique de l'Université de Montréal (CÉRAS), de l'Université Laval (CÉRUL), et de la Sûreté du Québec.

Résultats

Portrait des identités et activités virtuelles

Les identités virtuelles réfèrent aux informations personnelles inscrites par les cyberdélinquants sur leurs réseaux sociaux. Spécifiquement, nous nous sommes intéressés à l'âge et au nom que ceux-ci ont inscrit sur leurs profils virtuels, en plus des photos qu'ils y téléversent. Comme présenté au tableau 1, 32 (43,84 %) cyberdélinquants qui ont clavardé avec des jeunes (n = 73) se sont rajeunis, 41 (56,16 %) ont inscrit leur âge véritable, et aucun (0 %) ne s'est vieilli. Parmi ceux qui ont menti à propos de leur âge (n = 32), un peu moins de la moitié (46,88 %) ont prétendu être âgés en deçà de 18 ans et l'écart moyen entre leur âge véritable et celui allégué était de 18,80 ans (É.-T. = 13,10 ; étendue 3-45). L'autre moitié (53,13 %) prétendaient plutôt être d'âge majeur, le réduisant néanmoins. Leur écart moyen d'âge était de 14,46 ans (É.-T. = 14,47 ; étendue 4-33). Quant au nom utilisé, 25 (40,32 %) cyberdélinquants pour qui l'information était disponible (n = 62) ont fait l'usage d'un faux nom (ou pseudonyme), 13 (20,97 %) ont utilisé un pseudonyme similaire à leur nom véritable (p.ex., Nick pour Nicolas), et 24 (38,71 %) ont fourni leur nom véritable. Parmi ceux qui ont utilisé une photo de profil, 16 (51,61 %) cyberdélinquants pour qui l'information était disponible (n = 31) montraient leur véritable visage. En moyenne, ceux qui ont eu recours à des stratégies de protection de leur identité dans le cadre de leurs activités de sollicitation sexuelle de personnes mineures (n = 40) ont utilisé entre 1 et 2 stratégies (x = 1,78 ; É.-T. = 0,80 ; étendue = 1-3).

Tableau 1 :
Identités virtuelles et stratégies de protection de l'identité des cyberdélinquants

Caractéristiques des profils	Statistiques
Âge (n = 73)	
S'est rajeuni	32 (43,84 %)
Moins 18 ans	15 (46,88 %) Écart d'âge x = 18,80 (É.-T. = 13,10 ; étendue 3-45)
18 ans et +	17 (53,13 %) Écart d'âge x = 14,46 (É.-T. = 14,47 ; étendue 4-33)
A indiqué son âge	41 (56,16 %)
S'est vieilli	0 (0 %)
Nom (n = 62)	
Pseudonyme inventé	25 (40,32 %)
Similaire	13 (20,97 %)
Réel	24 (38,71 %)
Photo (n = 31)	
Présente son visage	16 (51,61 %)
Nombre de stratégies* (n = 40)	x = 1,78 (É.-T. = 0,80 ; étendue = 1-3)

Note : * Les stratégies de protection de l'identité incluent : s'être rajeuni, avoir indiqué un nom inventé, et ne pas avoir présenté son visage véritable

À propos des activités virtuelles des cyberdélinquants, nous avons examiné les stratégies employées pour protéger et préserver l'anonymat, les types de plateformes de clavardage utilisées pour communiquer avec les jeunes et les outils utilisés pour faire l'acquisition de pédopornographie à l'occasion du crime répertorié. Tel que présenté au tableau 2, 31 (19,25 %) cyberdélinquants de l'échantillon complet (*n* = 161) ont commis leurs infractions par l'entremise d'un ordinateur ou d'une connexion Wi-Fi publics, 25 (15,53 %) ont eu recours à du chiffrement pour protéger leurs systèmes informatiques et 7 (4,35 %) ont utilisé des proxys, VPN ou le Dark Web pour y détourner leurs adresses IP. Il est important de souligner qu'une grande majorité (64,60 %) n'a toutefois utilisé aucune stratégie de protection de leurs systèmes informatiques. En moyenne, ceux qui ont eu recours à ce type de stratégies (*n* = 57) ont utilisé entre 1 et 2 stratégies (x = 1,12 ; É.-T. = 0,33 ; étendue = 1-2).

Tableau 2 :
Les stratégies de protection des systèmes informatiques utilisées par les cyberdélinquants (n = 161)

Mesures de protection	Statistiques
Aucune stratégie	104 (64,60 %)
Ordinateur / WiFi public	31 (19,25 %)
Chiffrement	25 (15,53 %)
Proxy / VPN / Dark Web	7 (4,35 %)
Nombre de stratégies (n = 57)	x = 1,12 (É.-T. = 0,33 ; étendue = 1-2)

Les applications et plateformes utilisées par les délinquants ont aussi été examinées en fonction des critères liés aux profils, à la nature des contacts aux autres internautes, et des traces numériques laissées. Comme présenté au tableau 3, 46 (68,66 %) cyberdélinquants qui ont clavardé avec des jeunes et pour qui l'information était disponible (*n* = 67) ont utilisé une ou plusieurs plateformes à profils détaillés sur lesquelles plusieurs informations personnelles permettant l'identification peuvent être inscrites, notamment le nom, l'âge, le lieu de résidence, la profession, le niveau d'éducation, en plus d'une photo pouvant être téléversée (p.ex., Facebook, Doyoulookgood.com, Jasez.ca) et 56 (83,58 %) ont eu recours à d'autres applications à profils limités sur lesquels seulement un pseudonyme est requis (p.ex., mIRC, Omegle). Concernant la nature des contacts aux autres internautes, 59 (88,06 %) cyberdélinquants ont utilisé des plateformes et des applications exigeant l'approbation des utilisateurs, notamment par l'ajout « d'amis » au répertoire de contacts, pour entamer une discussion (p.ex., Facebook) et 46 (68,66 %) en ont utilisé d'autres permettant la communication immédiate avec des personnes inconnues (p.ex., mIRC, Omegle, Jasez.ca, Kik). Enfin, 37 (55,22 %) cyberdélinquants ont eu recours à des applications utilisant la technologie audio-vidéo synchrone, dont les traces numériques peuvent être qualifiées de volatiles. En moyenne, les cyberdélinquants ont utilisé entre 2 et 3 applications de clavardage (x = 2,34 ; É.-T. = 1,21 ; étendue = 1-6).

Tableau 3 :
Les caractéristiques des plateformes de clavardage utilisées par les cyberdélinquants (n = 67)

Caractéristiques des plateformes	Statistiques
Profils détaillés	46 (68,66 %)
Profils limités	56 (83,58 %)
Contact avec internautes connus	59 (88,06 %)
Contact avec étrangers	46 (68,66 %)
Technologie audio-vidéo en temps synchrone	37 (55,22 %)
Nombre de plateformes utilisées	x = 2,34 (É.-T. = 1,21 ; étendue = 1-6)

Le tableau 4 présente les caractéristiques des plateformes et des applications de clavardage contemporaines les plus utilisées par les cyberdélinquants, soient celles utilisées par les cyberdélinquants entre 2015 et 2020. Ainsi, les plus utilisées partagent la même caractéristique, à savoir qu'elles permettent les communications audiovisuelles en temps synchrone, laissant ainsi que peu de traces numériques liées à de potentielles infractions.

Tableau 4 :
Plateformes / applications de clavardage contemporaines (2015-2020) les plus utilisées et leurs caractéristiques

	Occurrence	Profil détaillé	Profil limité	Contact internautes connus	Contact étranger	Techno audio-vidéo
Facebook Messenger	9	x		x		x
Skype	4		x	x		x
SnapChat	3		x			x
mIRC	1		x		x	
Jasez.ca	1	x			x	
Badoo	1	x			x	
Yellow	1		x		x	
Kik	1	x		x	x	
Discord	1		x		x	x

Nous avons également examiné la source d'acquisition de pédopornographie lors du crime répertorié. Comme présenté au tableau 5, 67 (54,03 %) cyberdélinquants qui ont téléchargé de la pornographie juvénile (*n* = 124) l'ont fait à partir de logiciels de partage poste-à-poste (p.ex., Utorrent, E-mule, Shearaza), constituant la principale source de l'échantillon. Ensuite, 27 (21,77 %) cyberdélinquants ont effectué des recherches en sources ouvertes soit par l'entremise de moteurs de recherche traditionnels (p.ex., Google), de forums de discussions dédiés à la sexualisation des enfants ou de sites pornographiques traditionnels. D'autres se sont procuré le matériel dans un contexte interactionnel, soit 25 (20,16 %) cyberdélinquants ayant fait l'acquisition de ce matériel par l'entremise de leurs correspondances virtuelles avec leurs victimes ou d'autres internautes. Finalement, 4 (3,23 %) cyberdélinquants ont eux-mêmes produit leur matériel (p.ex., a filmé ses propres abus, a installé une caméra cachée dans une salle de bain) alors que 4 (3,23 %) ont eu recours au Dark Web (p.ex., Tor). En moyenne, les cyberdélinquants ont utilisé 1,24 source différente (É.-T. = 0,51 ; étendue = 1-3).

Tableau 5 :
Sources d'acquisition de pédopornographie lors du crime répertorié (n = 124)

Sources	Statistiques
Logiciel pair à pair (poste-à-poste)	67 (54,03 %)
Source ouverte	27 (21,77 %)
Correspondances virtuelles	25 (20,16 %)
Production artisanale	4 (3,23 %)
Dark Web	4 (3,23 %)
Nombre de sources	x = 1,24 (É.-T. = 0,51 ; étendue = 1-3)

Le tableau 6 présente les sources d'acquisition du matériel de pornographie juvénile par année, pour les cinq dernières années des crimes répertoriés. On remarque une tendance similaire entre les crimes contemporains et les anciens quant à la fréquence d'utilisation des sources d'acquisition du matériel, les logiciels poste-à-poste demeurant la principale source utilisée par les cyberdélinquants. Au cours des cinq dernières années, 19 (51,35 %) consommateurs de pornographie juvénile ont eu recours aux logiciels poste-à-poste, 8 (21,62 %) ont effectué des recherches en sources ouvertes, 14 (37,84 %) ont obtenu leur matériel de séances de clavardage et 3 (8,11 %) ont utilisé le Dark Web. Notons que si les logiciels

poste-à-poste font toujours partie des habitudes de téléchargement des cyberdélinquants, pratiquement tous les cas d'utilisation du Dark Web identifiés dans notre l'échantillon font partie d'une criminalité contemporaine. À l'inverse, la production artisanale de pornographie juvénile s'inscrit plutôt dans une criminalité plus ancienne.

Tableau 6:
Sources d'acquisition de pédopornographie par année du crime répertorié

	Logiciel poste à poste	Source ouverte	Production artisanale	Clavardage	Dark Web	Nombre de dossiers
2019	1	0	0	1	0	2
2018	0	0	0	1	0	1
2017	4	1	0	5	2	9
2016	6	6	0	6	1	15
2015	8	1	0	1	0	10
Total 5 ans (%)	19 (51,35)	8 (21,62)	0 (0)	14 (37,84)	3 (8,11)	37
Total échantillon (%)	69 (55,65)	27 (21,77)	4 (3,23)	26 (20,97)	4 (3,23)	124

Les stratégies de protection et les paramètres du crime
Enfin, nous avons examiné l'hypothèse selon laquelle les mesures prises par les cyberdélinquants sexuels seraient influencées par les paramètres de leur criminalité. À cet effet, des études suggèrent que le jeune âge, associé à une plus grande prise de risque, serait associé à une insensibilité face à la détection policière (Kierkergaard, 2011; Quayle et Taylor, 2011). Les individus moins fréquemment confrontés au système de justice seraient également moins sensibles à une telle détection (Wolak et al., 2008). Enfin, on pourrait croire que la contemporanéité, marquée par une plus grande disponibilité des outils technologiques orientés vers la confidentialité des internautes, sera associée à l'utilisation de plus de stratégies visant à préserver l'anonymat.

Pour chaque cyberdélinquant, nous avons donc mesuré le nombre de stratégies de protection utilisées en considérant à la fois les stratégies de protection des systèmes informatiques et celles liées à l'identité, à savoir: 1) l'utilisation d'un ordinateur ou Wi-Fi public pour commettre des délits, 2) le recours à du chiffrement pour protéger le système informatique, 3) l'utilisation de proxys, VPN ou Dark Web pour détourner l'adresse IP, mais également la transmission de fausses informations personnelles à propos de

4) l'âge, 5) du nom et, 6) de l'apparence du visage. Comme présenté au tableau 7, la moitié des cyberdélinquants n'ont utilisé aucune stratégie (n = 81 ; 50,31 %), la moyenne s'établissant à 1,49 stratégies pour ceux qui en ont utilisées (É.-T. = 0,80 ; étendue = 1-4).

Utilisant cette mesure, nous avons d'abord examiné si la présence d'antécédents criminels influençait la propension à préserver l'anonymat. Les résultats des analyses de corrélation indiquent que l'utilisation de stratégies de protection est liée au nombre total de chefs de leurre d'enfants (r = 0,33, p < 0,01), de crimes sexuels hors ligne (r = 0,21, p < 0,01) et de crimes généraux (r = 0,16, p < 0,05). Aucune autre relation significative n'a été identifié en lien avec le nombre de chefs de pornographie juvénile, de crimes violents et de bris de conditions.

Nous avons ensuite examiné si l'âge des cyberdélinquants influençait la propension à préserver l'anonymat. Les résultats de l'analyse corrélationnelle n'ont indiqué aucun lien significatif. Enfin, nous avons examiné si le moment au cours duquel les crimes ont été commis influençait la propension à préserver l'anonymat. Les résultats de cette analyse corrélationnelle ont indiqué que la contemporanéité des crimes commis sur l'internet est inversement associée au nombre de stratégies de protection de l'identité (r = -0,30, p < 0,01). Autrement dit, plus le crime est contemporain, moins de stratégies de protection de l'identité n'ont été employées.

Tableau 7 :
Influence des paramètres du crime sur les stratégies de protection de l'identité et des systèmes informatiques

Paramètres	Statistiques
Nombre de stratégies de protection (n = 80)	x = 1,49 (É.-T. = 0,80 ; étendue = 1-4)
Liens à	
# leurre d'enfants	0,33**
# pornographie juvénile	0,12
# crimes sexuels hors ligne	0,21**
# crimes violents	0,14
# bris de conditions	0,08
# crimes généraux	0,16*
Âge des cyberdélinquants	0,43
Année des infractions sur internet	-0,30**

** p < 0,01 ; * p < 0,05

Discussion

Cette étude visait à mieux comprendre les profils et les activités virtuelles de subterfuges utilisés par les cyberdélinquants qui sollicitent à des fins sexuelles les jeunes et ceux qui consomment du matériel de pornographie juvénile. Un certain nombre d'observations générales se dégagent des résultats. D'une part, les résultats indiquent qu'une proportion légèrement plus faible d'hommes mentent à propos de leur identité, en comparaison à ceux qui fournissent des informations véridiques à propos d'eux. D'autre part, on observe que seule une minorité de cyberdélinquants sexuels utilisent des outils technologiques pour protéger leurs systèmes informatiques dans le but éventuel d'éviter une détection policière. Ces résultats suggèrent que les cyberdélinquants mentent beaucoup moins qu'on pourrait s'y attendre et qu'ils n'emploient que très peu de moyens pour éviter la détection. Ce constat laisse d'ailleurs supposer que les subterfuges sont davantage orientés vers la séduction et la mise en confiance des victimes que vers la prévention de la détection policière.

Dans la même veine, les données montrent que les hommes qui clavardent avec des jeunes à des fins sexuelles sont autant présents sur les plateformes offrant la possibilité d'y fournir un profil détaillé que sur les plateformes à profil limité. Pour ces hommes, les technologies de communication audiovisuelle en temps synchrone étaient l'une des composantes des applications de clavardage les plus utilisées au cours des récentes années, alors que l'utilisation du Dark Web caractérisait une nouvelle tendance, quoi que peu prévalente dans les données policières, chez les hommes qui consomment de la pornographie juvénile. Ainsi, il semble clair que les traces numériques laissées par les cyberdélinquants demeurent assez substantielles.

Qu'est-ce qui influence l'utilisation de stratégie de préservation de l'anonymat en ligne ?

Un autre objectif de cette étude visait à examiner les paramètres du crime influençant la propension à préserver l'anonymat en ligne lors de délits sexuels. Les résultats ont montré que l'engagement dans la criminalité, et plus particulièrement le fait de s'être engagé dans plus de crimes sexuels à contact direct (virtuel ou hors ligne), était associé à l'utilisation de plus de stratégies de protection par les cyberdélinquants sexuels. Ce résultat est cohérent avec les études qui ont montré que les délinquants qui ont été plus fréquemment confrontés au système de justice étaient plus sensibles aux risques associés à leurs comportements délictueux (Wolak et al., 2008). Il est par ailleurs possible que le fait d'entrer en interaction avec une victime, ajoutant ainsi au risque d'être détecté celui d'être dénoncé, ait sensibilisé les cyberdélinquants à prendre plus de protection afin de préserver l'anonymat.

Contrairement à l'hypothèse selon laquelle les jeunes, dont le mode de vie se caractérise par la prise de risque, les résultats de cette étude ont montré qu'il n'existait pas d'association entre l'âge des cyberdélinquants sexuels

et leur propension à préserver l'anonymat en ligne. Le jeune âge ne semble donc pas associé à la prise de risque ni plus que l'expérience acquise avec l'âge ne semble associée à une certaine retenue. La motivation sexuelle, plus intrinsèque et dirigée vers les personnes mineures, pourrait plutôt expliquer cet état de fait. Enfin, nous avons émis l'hypothèse selon laquelle la contemporanéité, marquée d'un plus grand accès aux outils technologiques, serait associée à l'utilisation de plus de stratégies de protection. Encore, nos résultats ont infirmé cette hypothèse. Ils ont plutôt montré que l'ancienneté des dossiers était associée à l'utilisation de telles stratégies. Ce résultat est toutefois cohérent avec l'étude de Wolak et ses collaborateurs (2011) qui ont observé une proportion à la baisse des cyberdélinquants qui ont utilisé des méthodes de chiffrement entre 2000 et 2006. La désindividuation créée par la virtualité de l'internet qui favorise les comportements impulsifs et désinhibés (Prichard et al., 2011) et le fait de croire que l'univers virtuel n'est pas la réalité (Paquette et Cortoni, 2020) pourraient également expliquer pourquoi certains cyberdélinquants sexuels ignorent les risques associés à leur cybercriminalité.

Les profils trompeurs et véridiques des auteurs de leurre

Dans cette étude, un peu moins de la moitié des hommes qui ont communiqué en ligne avec des jeunes à des fins sexuelles ont adopté une identité virtuelle trompeuse, mentant le plus souvent à propos de leur nom et âge. Ces hommes étaient présents tant sur les plateformes à profils détaillés et que limités. En rapport aux hommes qui fournissent des informations personnelles véridiques, cette plus faible portion coïncide avec les études qui observent une tendance semblable (p.ex., Briggs et al., 2011). Tel que suggéré par des chercheurs, le mensonge à propos de ses informations personnelles pourrait non seulement permettre de préserver l'anonymat dans le but d'éviter la détection policière, mais une personnification plus jeune pourrait également permettre de séduire les jeunes et les mettre en confiance afin qu'ils s'adonnent dans des conversations ou échanges à caractère sexuel (O'Malley et Holt, 2020). Dans notre échantillon, tous les hommes qui ont menti à propos de leur âge l'ont fait en se rajeunissant, mais seulement un peu moins de la moitié l'ont fait au moins de prétendre être d'âge similaire à celui des adolescents.

À l'inverse, plusieurs cyberdélinquants ont allégué un âge adulte plus près du leur et plus de la moitié de l'échantillon ont transmis leur âge véritable. Ils ont également été nombreux à indiquer leur nom véritable et téléverser une photo de leur visage. Alors que cette stratégie est intuitivement incohérente à l'idée de préserver l'anonymat à l'occasion d'activités illégales, plusieurs hypothèses permettent d'expliquer cette décision. D'une part, il est possible que ces hommes soient si absorbés par leurs activités sexuelles qu'ils négligent les risques associés à leurs sollicitations. Cette hypothèse serait cohérente avec les résultats de l'étude de Webster et ses collaborateurs (2012) qui ont trouvé que les cyberdélinquants utilisant le moins de stratégies de protection de l'identité étaient des hommes dont la sexualité

est envahissante et régulation des comportements déficitaire. Typiquement, ces hommes ne perçoivent ni le caractère répréhensible de leurs gestes et, conséquemment, ni l'utilité de cacher des informations à propos d'eux (Balfe et al., 2015 ; Webster et al., 2012). D'autre part, pour les cyberdélinquants sexuels désireux d'obtenir une rencontre hors ligne et de s'adonner à des contacts sexuels avec leurs victimes, il est possible que le fait de mentir sur son âge, à tout le moins de manière exagérée, compromette le lien de confiance qu'ils ont établi au cours des échanges virtuels, réduisant ainsi la probabilité d'actualiser les contacts sexuels. Cette hypothèse fait échos à la typologie proposée par Briggs et ses collaborateurs (2011) qui distinguent les cyberdélinquants uniquement motivés par les fantaisies sexuelles en ligne des cyberdélinquants motivés par la perspective de contacts sexuels hors ligne. Dans notre étude, le mensonge à propos de l'identité est possiblement au service des cyberdélinquants motivés par les fantaisies sexuelles en ligne alors que la transmission d'informations personnelles serait au service des rencontres hors ligne. Ne disposant toutefois pas des données nécessaires pour soutenir ces hypothèses, des études futures seraient nécessairement pour les confirmer ou infirmer.

Les outils technologies des consommateurs de pornographie juvénile

Les résultats ont montré que près des deux tiers des cyberdélinquants de notre échantillon n'ont utilisé aucune stratégie de protection de leurs systèmes informatiques et la quasi-totalité des consommateurs de pornographie juvénile a fait l'acquisition de leur matériel par l'entremise d'outils laissant des traces numériques en lien avec leurs adresses IP. Par ailleurs, alors que l'utilisation du Dark Web a été utilisé à l'occasion des crimes les plus récents, nos données ont montré que le poste-à-poste est toujours l'outil d'acquisition de pédopornographie le plus populaire (Kierkergaard, 2011 ; Wolak et al., 2014), et que des technologies délaissées par le grand public (p.ex., mIRC) étaient toujours utilisées par les cyberdélinquants sexuels (Balfe et al., 2015).

La tendance à la non-utilisation de stratégies de protection des systèmes informatiques peut s'expliquer fort probablement par le manque de connaissances techniques des cyberdélinquants, mais il est également possible que nombre d'entre eux perçoivent que l'internet offre à lui seul un anonymat suffisant, minimisant ainsi le risque d'être détecté par la police (Balfe et al., 2015). Au même titre que les hommes qui s'engagent dans des communications à caractère sexuel avec des mineurs en ligne, il est possible que leur sexualité et leur autorégulation problématique nuisent à l'évaluation qu'ils font des risques associés à leurs comportements délictueux.

Toutefois, considérant la faible propension à l'utilisation de proxys, VPN ou du Dark Web, il est également possible que les cyberdélinquants les plus prudents aient échappé à la détection policière et, conséquemment, n'aient pas été inclus dans notre échantillon. À cet effet, des auteurs suggèrent que les cyberdélinquants qui échappent à la détection policière seraient ceux

qui conserveraient leurs contenus numériques illégaux sur des serveurs hébergés dans des pays dont les lois n'encadrent pas la pornographie juvénile ou ceux dont les activités virtuelles se dérouleraient sur des sites et plateformes web non dédiés à la sexualisation des enfants, lesquels seraient moins surveillés par les autorités policières (Balfe et al., 2015 ; Kierkergaard, 2011 ; Mitchell et al., 2005 ; Steel, 2009). Afin de mieux comprendre les stratégies de subterfuges efficaces des cyberdélinquants qui échappent à la détection policière, des devis de recherche différents seront toutefois nécessaires.

Limites et perspectives pour la recherche future

Un certain nombre de limites de cette étude doivent être soulignées. D'abord, l'utilisation de données policières entraîne intrinsèquement un biais de sélection. La police détecte les cas les plus visibles puisque les dossiers résultent de plaintes ou détections proactives. Un cyberdélinquant qui emploie toutes les stratégies pour préserver son anonymat a manifestement moins de chances de se faire arrêter et, conséquemment, de se retrouver parmi les sujets de notre étude. Celle-ci demeure toutefois pertinente dans la mesure où elle rend compte de l'utilisation des subterfuges par les individus qui ont fait l'objet de la détection, soulignant ainsi que la police ne détecte que la pointe de l'iceberg, la plus visible. Afin d'élargir les connaissances à propos des pratiques de préservation de l'anonymat des cyberdélinquants qui échappent à la détection policière, l'étude des forums de discussion dédiés à la sexualisation des enfants, notamment sur le Dark Web, pourrait s'avérer une avenue prometteuse.

Les dossiers sous étude incluent aussi des personnes arrêtées ayant œuvré dans un réseau structuré de cyberdélinquants qu'on associe à une plus grande connaissance technique. Considérant la taille de l'échantillon, il n'était pas possible de comparer les pratiques virtuelles des cyberdélinquants solitaires à celles des cyberdélinquants qui œuvraient en interaction avec d'autres internautes. Les recherches futures pourraient ainsi bénéficier d'une analyse approfondie de l'impact de la sollicitation entre cyberdélinquants sur la technicité numérique et les pratiques de préservation de l'anonymat.

Ensuite, nous avons uniquement pu étudier la technologie utilisée dans le contexte du crime répertorié. Une analyse plus exhaustive des outils installés sur les disques durs des cyberdélinquants aurait peut-être permis de découvrir d'autres outils technologiques de protection de l'anonymat utilisés antérieurement ou pour d'autres fins.

Finalement, l'étude a permis d'établir des liens entre les comportements observés et les cognitions des cyberdélinquants sur la base de dossiers policiers. Avec un accès direct aux cyberdélinquants sexuels, des analyses psychologiques et psychométriques permettraient potentiellement d'obtenir des informations supplémentaires quant à leurs perceptions sur les subterfuges, la nature des données policières ne permettant malheureusement pas d'obtenir ce genre d'information.

Implications et conclusion

Cette étude avait pour objectif d'examiner les identités virtuelles, le mensonge et les pratiques de préservation de l'anonymat des hommes qui utilisent l'internet et les réseaux sociaux pour solliciter des jeunes à des fins sexuels et faire l'acquisition de matériel de pornographie juvénile. Les résultats ont montré des pratiques variées quant à la divulgation d'informations personnelles dans le cadre de communications sexuelles en ligne et au recours aux techniques numériques d'anonymisation des systèmes informatiques dans le cadre d'acquisition de pédopornographie. Les résultats ont aussi montré une tendance maintenue quant à l'utilisation des logiciels poste-à-poste, mais également une nouvelle tendance orientée vers l'utilisation des technologies ne laissant que peu de traces numériques par les cyberdélinquants sexuels.

En plus de contribuer aux connaissances scientifiques, les résultats de cette étude ont des implications concrètes pour la pratique policière alors qu'ils mettent en lumière les lieux contemporains exploités par les cyberdélinquants sexuels, permettant ainsi d'orienter les enquêtes virtuelles proactives de manière conséquente. Au-delà de la perspective d'identifier des cyberdélinquants sexuels, la mise en relation des paramètres de la criminalité suggère des pistes à considérer pour la priorisation des dossiers à enquêter. À titre d'exemple, sachant que la présence d'un historique criminel, reconnu en criminologie comme étant un facteur de risque de récidive (Hanson et Morton-Bourgon, 2005), est associée à une utilisation plus importante de stratégies de préservation de l'anonymat, il serait ainsi pertinent de considérer de manière prioritaire les dossiers dans lesquels les traces numériques laissées par les cyberdélinquants suggèrent qu'ils mentent à propos de leur identité. Par ailleurs, sachant que les cyberdélinquants sexuels utilisent souvent plusieurs plateformes virtuelles pour leurs activités délictuelles, il pourrait s'avérer pertinent de mener de front les enquêtes tant sur le Clearnet que sur le Dark Web. Le croisement des traces numériques provenant de ces deux sources pourrait certainement augmenter la probabilité d'intercepter les cyberdélinquants utilisant les stratégies les plus sophistiquées pour éviter la détection policière.

Des implications pratiques en termes de prévention de la victimisation des enfants et adolescents sont également à souligner. Si une présence policière plus active sur les réseaux virtuels de prédilection des cyberdélinquants pourrait contribuer à réduire la victimisation sexuelle, un travail de prévention, en amont, devrait également être privilégié auprès des enfants, des adolescents et de leurs parents. Avec l'accessibilité aux appareils électroniques et la mouvance quant aux plateformes utilisées par les jeunes, des programmes de sensibilisation destinés aux parents devraient être élaborés afin qu'ils demeurent à l'affût des activités virtuelles des jeunes. Similairement, d'autres programmes devraient spécifiquement cibler la clientèle vulnérable, les jeunes, afin de les sensibiliser aux risques inhérents associés

à leurs activités en ligne, mais aussi aux stratégies utilisées par les cyberdélinquants pour les engager dans des communications ou comportements sexuels en ligne et hors ligne.

En conclusion, cette étude offre, à partir de données préliminaires, un portrait des identités et pratiques virtuelles des cyberdélinquants sexuels qui ciblent les enfants et les adolescents. Malgré ces nouvelles connaissances, il reste encore beaucoup de zones à explorer pour les chercheurs. La multiplication des efforts de recherche pourra nécessairement contribuer à l'amélioration des pratiques d'intervention et de prévention, et ainsi lutter à réduire cette forme de forme de criminalité numérique.

Références

Babchishin, K. M., Hanson, R. K. et Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. Sexual Abuse: *A Journal of Research and Treatment, 23*, 92-123. 10.1177/1079063210370708

Babchishin, K. M., Hanson, R. K. et VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behaviour, 44*, 45-66. 10.1007/s10508-014-0270-x

Balfe, M., Gallagher, B., Masson, H., Balfe, S., Brugha, R. et Hackett, S. (2015). Internet child sex offenders' concerns about online security and their use of identity protection technologies: A review. *Child Abuse Review, 24*, 427-439. 10.1002/car.2308

Beech E., Birgden, A. et Findlater, D. (2008). The internet and child sexual offending: A criminological review. *Aggression and Violent Behaviour, 13*, 216–228. 10.1016/j.avb.2008.03.007

Briggs, P., Simon, W. T. et Simonsen, S. (2011). An exploratory study of internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender? *Sexual Abuse: A Journal of Research and Treatment, 23*, 72–91. 10.1177/1079063210384275

Cooper, A. (1998). Sexuality and the internet: Surfing its way into the New Millennium. *CyberPsychology & Behavior, 1*, 187-193. 10.1089/cpb.1998.1.187

Cooper, A. (2002). *Sex and the Internet: A Guidebook for Clinicians.* Brunner-Routledge.

Cyberaide (2016). Les images d'abus pédosexuels sur internet : une analyse de Cyberaide.ca. Canada : Centre canadien de protection de l'enfance. www.cyberaide.ca/pdfs/CTIP_CSAResearchReport_Summary_2016_fr.pdf

D'Ovidio, R., Tyson, M., Imanni, J. et Shumar, W. (2009). Adult-child sex advocacy websites as social learning environments: A content analysis. *International Journal of Cyber Criminology, 3,* 421-440.

Dowdell, E. B., Burgess, A. W. et Flores, J. R. (2011). Online social networking patterns among adolescents, young adults, and sexual offenders. *The American Journal of Nursing, 111*, 28-36. 10.1097/01.NAJ.0000399310.83160.73

Eke, A. W., Seto, M. C. et Williams, J. (2011). Examining the criminal history and future offending of child pornography offenders: An extended prospective follow-up study. *Law and Human Behavior, 35*, 466-478. 10.1007/s10979-010-9252-2

Eneman, M. (2009). Counter-surveillance strategies adopted by child pornographers. *International Journal of Technology and Human Interaction, 5*, 1–17. 10.4018/jthi.2009062501

Fortin, F., Paquette, S. et Dupont, B. (2017). De la pornographie légale à l'agression sexuelle : les scripts des activités à caractère pédophile sur Internet. *Criminologie, 50*, 200-227. 10.7202/1039802ar

Gehl, R.-W. (2016). Power/freedom on the darknet: A digital ethnography of the Dark Social Network. *New Media & Society, 18*, 1219-123. 10.1177/1461444814554900

Glasgow, D. (2010). The potential of digital evidence to contribute to risk assessment of internet offenders. *Journal of Sexual Aggression, 16*, 87–106. 10.1080/13552600903428839

Graham, R. et Pitman, B. (2018). Freedom in the wilderness: A study of a Darknet space. *Convergence: The International Journal of Research into New Media Technologies, 26*, 1-27. 10.1177/1354856518806636

Graham, W. (2000). Uncovering and eliminating child pornography rings on the internet: issues regarding and avenues facilitating law enforcement's access to 'Wonderland'. *Law Review of Michigan State University, 2*, 457–484.

Haasz, A. (2016). Underneath it all: Policing international child pornography on the Dark Web. *Syracuse Journal of International Law and Commerce, 43*, 353-380.

Hanson, R. K. et Morton-Bourgon, K. E. (2005). The characteristics of persistent sexual offenders: A meta-analysis of recidivism studies. *Journal of Consulting and Clinical Psychology, 73*, 1154-1163. 10.1037/0022-006X.73.6.1154

Holt, T., Kristie, B. et Burker, N. (2010). Considering the pedophile subculture online. *Sexual Abuse: A Journal of Research and Treatment, 22*, 3-24. 10.1177/1079063209344979

Kierkergaard, S. (2011). To block or not to block: European child porno law in question. *Computer Law and Security Review, 27*, 573–584. 10.1016/j.clsr.2011.09.005

Krone, T. (2005). A typology of online child pornography offending. *Trends & Issues in Crime and Criminal Justice (Australian Institute of Technology)*, 279. aic.gov.au/publications/tandi/tandi279

Liberatore, M., Erdely, R., Kerle, T., Levine, B. et Shields, C. (2010). Forensic investigation of peer-to-peer file-sharing networks. *Digital Investigation, 7*, s95–s103. 10.1016/j.diin.2010.05.012

Mitchell, K. J., Finkelhor, D., Jones, L. M. et Wolak, J. (2010). Growth and change in undercover online child exploitation investigations, 2000–2006. *Policing and Society, 20*, 416-431. 10.1080/10439463.2010.523113

Nunnally, J. C. et Berstein, I. H. (1994). *Psychometric Theory (3rd ed.).* McGraw-Hill.

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.* Prépublication. 10.1177/0886260520909186

Owen, G. et Savage, N. (2015). The Tor Dark Net. *Paper series, number 20*. https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf.

Paquette, S. et Cortoni, F. (2020). Offense-supportive cognitions expressed by men who use internet to sexually exploit children: A thematic analysis. *International Journal of Offender Therapy and Comparative Criminology.* Prépublication. 10.1177/0306624X20905757

Prat, S., Bertsch, I., Chudzik, L. et Réveillère, C. (2014). Women convicted of a sexual offence, including child pornography production: Two case reports. *Journal of Forensic and Legal Medicine, 23*, 22-24. 10.1016/j.jflm.2014.01.002

Prichard, J., Watters, P. et Spiranovic, C. (2011). Internet subcultures and pathways to the use of child pornography. *Computer Law and Security Review, 27*, 585–600. 10.1016/j.clsr.2011.09.009

Quayle, E. et Taylor, M. (2011). Social networking as a nexus for engagement and exploitation of young people. *Information Security Technical Report, 16*, 44–50. 10.1016/j.istr.2011.09.006

Ray, J., Kimonis, E. et Donoghue, C. (2010). Legal, ethical, and methodological considerations in the internet-based study of child pornography offenders. *Behavioral Sciences and the Law, 28*, 84–105. 10.1002/bsl.906

Seto, M., Reeves, L. et Jung, S. (2010). Explanations given by child pornography offenders for their crimes. *Journal of Sexual Aggression, 16*, 169–180. 10.1080/13552600903572396

Seto, M. C. (2013). *Internet Sex Offenders.* American Psychological Association.

Seto, M. C., Hanson, R. K. et Babchishin, K. M. (2011). Contact sexual offending by men with online sexual offenses. *Sexual Abuse: A Journal of Research and Treatment, 23*, 124-145. 10.1177/1079063210369013

Seto, M. C., Wood, J. M., Babchishin, K. M. et Flynn, S. (2012). Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders. *American Psychological Association, 36*, 320-330. 10.1037/h0093925

Sheehan, V. et Sullivan, J. (2010). A qualitative analysis of child sex offenders involved in the manufacture of indecent images of children. *Journal of Sexual Aggression, 16*, 143–167. 10.1080/13552601003698644

Solon, O. (2020, 17 juillet). *Inside the surveillance software tracking child porn offenders across the globe.* NBC news. https://www.nbcnews.com/tech/internet/inside-surveillance-software-tracking-child-porn-offenders-across-globe-n1234019

Steel, C. (2009). Child pornography in peer-to-peer networks. *Child Abuse & Neglect, 33*, 560–568. 10.1016/j.chiabu.2008.12.011

Statista, (2021, 24 mars). Most popular social networks worldwide as of January 2021, ranked by number of active users. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

U.S. Department of Justice. (2010). *The national strategy for child exploitation prevention and interdiction: A report to Congress.* Washington, DC: Author.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham T … Craparo, G. (2012). *European online grooming project. Final report.* natcen.ac.uk/media/22514/european-online-grooming-projectfinalreport.pdf

Wolak, J., Finkelhor, D., Mitchell, K. et Ybarra, M. (2008). Online predators and their victims: Myths, realities and implications for prevention and treatment. *American Psychologist, 63,* 111–128. 10.1037/0003-066X.63.2.111

Wolak, J., Finkelhor, D. et Mitchell, K. (2011). Child pornography possessors: Trends in offender and case characteristics. *Sexual Abuse: A Journal of Research and Treatment, 23*, 22–42. 10.1177/1079063210372143

Wolak, J., Finkelhor, D. et Mitchell, K. J. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health, 35*, 424. e11-424.e20

Wolak, J., Liberatore, M. et Levine, B. N. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect, 38*, 347–356. 10.1016/j.chiabu.2013.10.018

Wortley, R. K. et Smallbone, S. (2006). *Child pornography on the internet: Problem-oriented guides for police problem-Specific guides series (Report No.41).* US Department of Justice. http://www.ncdsv.org/images/COPS_Child-Pornography-on-the-Internet_5-2006.pdf