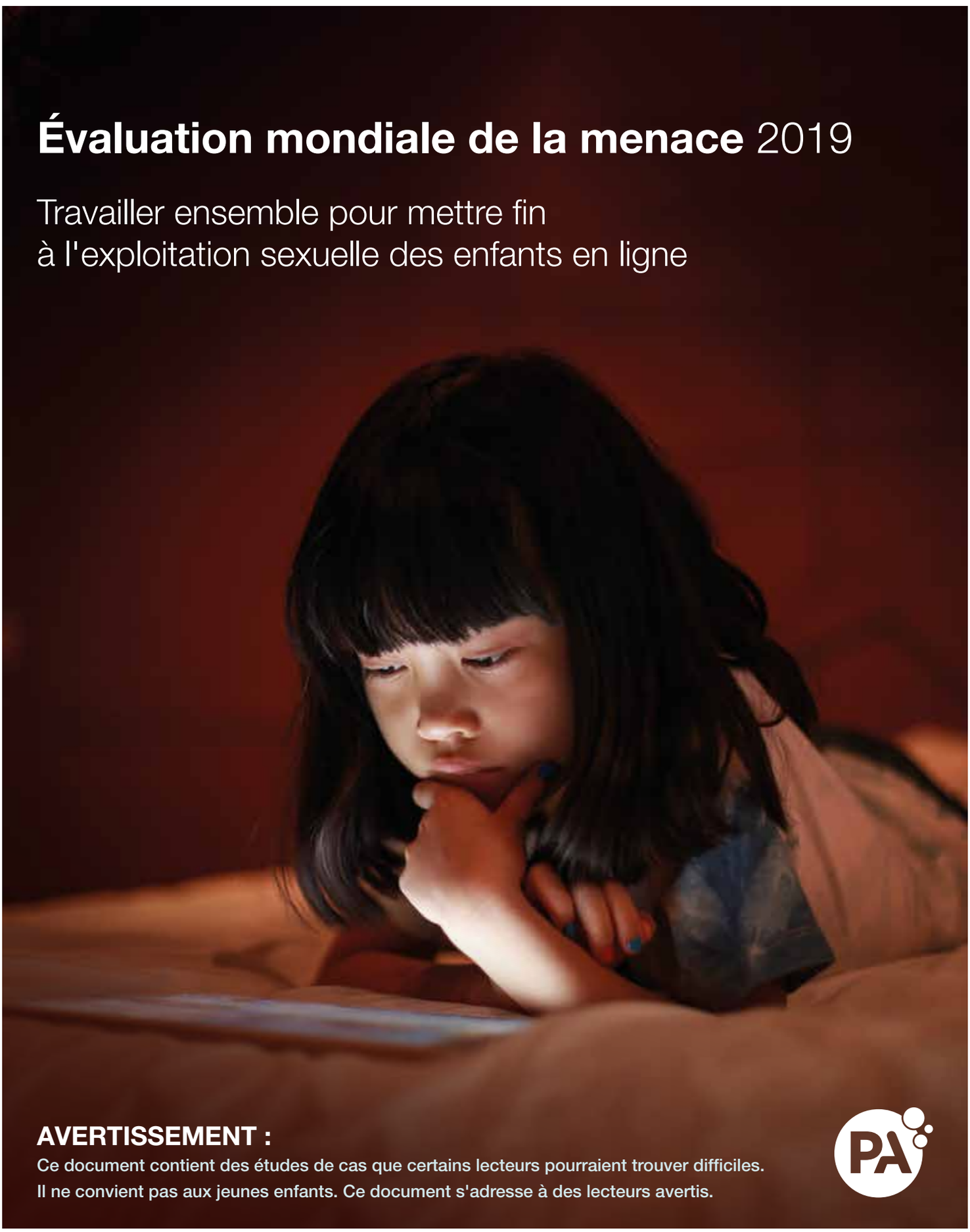
WePROTECT GLOBAL ALLIANCE

Évaluation mondiale de la menace 2019

Travailler ensemble pour mettre fin à l'exploitation sexuelle des enfants en ligne



AVERTISSEMENT :

Ce document contient des études de cas que certains lecteurs pourraient trouver difficiles. Il ne convient pas aux jeunes enfants. Ce document s'adresse à des lecteurs avertis.

Remerciements

WePROTECT Global Alliance souhaite remercier les organismes suivants pour leurs conseils spécialisés ainsi que PA Consulting Group pour leurs recherches et la préparation de ce rapport :

Aarambh Foundation (Inde)
ECPAT International
eSafety Commissioner (Australie)
Commission européenne
Europol
International Justice Mission
Internet Watch Foundation
INTERPOL
National Center for Missing and Exploited Children (États-Unis)
National Crime Agency (R-U)
The Global Partnership to End Violence Against Children
The Lucy Faithfull Foundation
UNICEF Ghana
US Department of Justice

Contenu

01 Avant-propos

par Ernie Allen, Président de WePROTECT Global Alliance

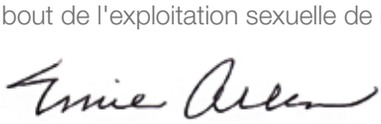
Lors de notre dernier sommet, co-organisé avec le Global Partnership to End Violence Against Children (Partenariat mondial pour mettre fin à la violence contre les enfants) et le gouvernement de Suède en 2018, WePROTECT Global Alliance a publié sa première évaluation mondiale de la menace. Il s'agissait de la première évaluation de ce type, réunissant des experts de l'Alliance afin de produire une analyse internationale et disponible pour tous de l'étendue et de la nature de la menace en ligne contre les enfants. L'objectif de cette évaluation était de renforcer notre réponse mondiale.

Grâce à PA Consulting, qui a soutenu l'évaluation de la menace de manière généreuse et pro bono, ainsi qu'à l'expertise et aux connaissances de nos membres, nous avons renforcé notre position et pris en compte les commentaires qui nous ont été adressés. Cette nouvelle version de l'évaluation de la menace apporte un nouveau regard sur la nature des abus sexuels contre les enfants en ligne dans le Sud. Elle aborde également les innovations technologiques qui auront un impact sur cette menace.

Nos conclusions sont inquiétantes. Nous constatons que l'étendue du problème, en termes absolus mais aussi en ce qui concerne les rapports qui émanent des services de répression et de la société civile, augmente de façon alarmante. Derrière chaque dossier se trouve un enfant qui a besoin de protection et d'assistance. Ce « raz-de-marée » d'affaires augmente la pression exercée sur chacun des piliers de WePROTECT Global Alliance : les gouvernements, les services de répression, la société civile et l'industrie des technologies. Au fur et à mesure que la connexion à Internet se répand, tout particulièrement dans le Sud, les délinquants localisent et exploitent de nouvelles victimes.

Dans le même temps, nous recevons de moins en moins de rapports car les méthodes de cryptage appliquées par l'industrie font que les entreprises technologiques sont de moins en moins capables d'identifier et de signaler l'utilisation malveillante de leurs propres plateformes. L'écart se creuse entre les nations qui ont eu le temps de développer des services d'assistance sophistiqués en parallèle avec leur évolution technique, et les nations qui adoptent la technologie tellement rapidement que leurs préparatifs ne sont pas à la hauteur. L'anonymat et les réseaux sécurisés permettent toujours aux délinquants de mettre en place des espaces en ligne sûrs, leur permettant de se mettre en contact les uns avec les autres et de diffuser des outils et des techniques qui favorisent l'exploitation. Le développement de nos connaissances quant à la méthodologie et à la motivation des délinquants ainsi qu'aux besoins et à l'impact sur les victimes des abus met en évidence l'importance de la prévention et de la protection. En clair, empêcher les abus avant qu'ils ne se produisent. Des estimations prudentes de l'impact financier de ces crimes s'élèvent à des milliards de dollars, en matière de santé, de services sociaux et d'impact sur la qualité de vie. Il existe une justification économique, opérationnelle et morale à ce que nous renforcions notre réponse.

Étant donné qu'un nombre grandissant d'enfants dans le monde accèdent à Internet et que l'environnement technologique évolue, nous avons besoin, aujourd'hui plus que jamais, d'un forum de collaboration, de réseautage et d'action. WePROTECT Global Alliance apporte une plateforme, une voix et un ensemble d'outils à ses membres pour combattre les abus sexuels contre les enfants en ligne à l'échelle internationale. En plus de cette évaluation de la menace, nous lançons également la réponse stratégique mondiale, qui établit une structure d'action au niveau transnational, grâce aux connaissances d'experts. Notre combat continue pour sensibiliser sur ce fléau, soutenir les actions pour enfin pouvoir venir à bout de l'exploitation sexuelle de nos enfants en ligne.



Ernie Allen
Président, Conseil de WePROTECT Global Alliance

Définitions et portée

WePROTECT Global Alliance (WPGA) est une coalition internationale dont l'objectif est d'exécuter des actions à l'échelle nationale et internationale pour mettre fin à l'exploitation sexuelle des enfants en ligne. Nous utilisons, dans le présent rapport, les termes et les abréviations suivantes :

CSEA (ou exploitation sexuelle des enfants en ligne) : L'exploitation et les abus sexuels d'enfants (également connus sous les abréviations anglaises CSAE et CSE) est une forme d'abus sexuels contre les enfants qui se produit lorsqu'un individu ou un groupe d'individus tire parti d'un déséquilibre du pouvoir pour forcer, manipuler ou tromper un enfant ou une personne de moins de 18 ans à effectuer un acte sexuel.

La victime peut avoir été sexuellement exploitée même si l'acte sexuel semble consensuel. L'exploitation sexuelle d'un enfant ne passe pas toujours pas un contact physique ; elle peut s'effectuer grâce à la technologie.[1]

WPGA cautionne la portée établie par la convention européenne sur la protection des enfants contre l'exploitation et les abus sexuels, également connue sous le nom de Convention de Lanzarote, qui vise à couvrir toutes les formes possibles d'infractions sexuelles contre des enfants, y compris les abus sexuels, l'exploitation par le biais de la prostitution, la sollicitation à des fin sexuelles et la corruption de mineurs via l'exposition à du contenu à caractère sexuel, ainsi que les activités et les infractions liées au matériel pédopornographique. La convention couvre également les abus sexuels au sein de la famille même de l'enfant (« le cercle de confiance ») ainsi que les abus commis pour des raisons commerciales ou dans un but lucratif. La Convention de Lanzarote établit les six infractions pénales suivantes :

- Article 18 : abus sexuels
- Article 19 : prostitution enfantine
- Article 20 : pornographie enfantine* [dans le présent rapport, ceci est identifié comme matériel pédopornographique]
- Article 21 : participation d'un enfant à des spectacles pornographiques
- Article 22 : corruption d'enfants
- Article 23 : sollicitation d'enfants à des fins sexuelles (ou « grooming en ligne »).

Matériel pédopornographique : Les agences des Nations Unies et d'autres institutions internationales décrivent les images et les vidéos indécentes d'enfants comme de la « pornographie enfantine ». Suite au projet du Groupe de travail interinstitutionnel et guide de terminologie, achevé en juin 2016, WPGA préconise l'utilisation de l'expression « matériel pédopornographique » car elle décrit avec précision la nature odieuse de la violence et de l'exploitation sexuelles des enfants tout en protégeant la dignité des victimes.

Le Nord et le Sud :
Pour faire la différence entre les différents niveaux de richesse et de développement parmi les pays membres, nous avons utilisé dans ce rapport l'expression « Nord » pour les pays du G8, les États-Unis, le Canada, tous les États membres de l'Union européenne, Israël, le Japon, Singapour, la Corée du Sud ainsi que l'Australie, la Nouvelle-Zélande et quatre des cinq membres permanents du Conseil de sécurité des Nations Unies, à l'exception de la Chine. Le « Sud » est composé de l'Afrique, de l'Amérique latine, du Moyen-Orient et de l'Asie émergente. Il comprend trois des quatre nouvelles économies avancées du BRIC (exception faite de la Russie) : Brésil, Inde et Chine.

Dans ce rapport, nous utilisons les termes « délinquant » et « agresseur » de manière indistincte pour définir les individus qui commettent l'exploitation sexuelle et les abus sexuels sur les enfants en ligne.

Nous avons aussi utilisé les expressions suivantes pour définir les différents types d'hébergement des services en ligne :

- le **Web visible** est la partie du Web qui est disponible au grand public et sur laquelle des recherches peuvent être menées avec des moteurs de recherche de base.
- le **Web profond** est la partie du Web dont le contenu n'est pas indexé par les moteurs de recherche de base. Elle est utilisée pour la messagerie Web, la banque en ligne et les services d'abonnement. On peut localiser et consulter le contenu avec une URL ou une adresse IP directe et cela peut nécessiter un mot de passe ou d'autres mesures de sécurité au-delà de la page Web publique.
- le **Dark Web** (ou Dark Net) est une expression litigieuse mais comprise par la plupart des autorités. Dans le contexte de ce rapport, nous l'entendons comme une couche d'informations et de pages auxquelles on ne peut accéder que par l'intermédiaire de « réseaux superposés (comme les réseaux privés virtuels ou VPN) et les réseaux de partage de fichiers pair à pair (ou P2P), qui dissimulent l'accès au public. Pour accéder au Dark Web, les utilisateurs ont besoin de logiciels spécifiques, car il est en grande partie crypté et les pages Web sont hébergées de manière anonyme.

02 Objectifs de l'évaluation mondiale de la menace

La première évaluation mondiale de la menace a été publiée en février 2018 et lancée lors du sommet du Programme 2030 pour mettre fin à la violence envers les enfants qui s'est tenu à Stockholm, en Suède. Il s'agissait de la première évaluation de ce type : un aperçu mondial et détaillé sur les évolutions technologiques, la vulnérabilité des victimes et le comportement des délinquants qui favorisent l'exploitation et les abus sexuels des enfants.

La conclusion principale de l'évaluation mondiale de la menace 2018 est que « les technologies permettent aux communautés de délinquants d'atteindre un niveau d'organisation sans précédent, ce qui pose une menace nouvelle et persistante car ces individus et ces groupes exploitent les « lieux sûrs » en ligne et ont accès « à la demande » aux victimes.[2]

Cette découverte éclairée est un appel aux armes pour les gouvernements afin qu'ils redoublent d'efforts pour identifier des méthodes à la fois nouvelles et innovantes contre cette menace qui pèse sur les personnes les plus vulnérables au sein de nos sociétés. Leur réponse inclut : le déploiement de capacités de renseignement sophistiquées pour interrompre les communautés de délinquants les plus dangereux, de meilleures ressources pédagogiques et d'assistance et des mesures législatives et réglementaires améliorant la surveillance des entreprises technologiques et clarifiant leur responsabilité en matière de protection des enfants en ligne via des actions robustes destinées à combattre les contenus et les activités illégaux.

90 pays déjà membres de WePROTECT Global Alliance

22 des plus grands noms de l'industrie technologique mondiale

26 organisations internationales et non-gouvernementales de premier plan

Cette année, le rapport a été préparé avec l'aide et l'expertise des membres du conseil de WePROTECT Global Alliance. Il s'inscrit dans la continuité du succès et de l'impact de l'évaluation mondiale de la menace 2018. Son objectif est de décrire la nature, l'étendue et la complexité de l'exploitation sexuelle des enfants en ligne pour soutenir une forte mobilisation, c'est-à-dire inciter les États membres, l'industrie technologique à l'échelle internationale et le secteur tertiaire à identifier de nouvelles manières de travailler ensemble pour combattre cette menace en rapide évolution. Le modèle de réponse nationale WePROTECT oriente et assiste les pays et les organisations à apporter une meilleure réponse à l'exploitation sexuelle des enfants en ligne.

L'évaluation part de la même optique que l'évaluation mondiale de la menace 2018 et conserve le même objectif (voir ci-dessous), avec une attention plus poussée et une meilleure compréhension de chacun des thèmes. Notre objectif est d'apporter une perspective plus internationale de la menace, qui prend en compte des contextes et des perspectives culturelles autres que celles des données et des études de cas de notre premier rapport, basées sur l'Amérique du Nord et l'Europe de l'Ouest. Ce rapport a pour but de :

- renforcer notre travail de sensibilisation à l'échelle internationale et de mieux comprendre l'exploitation sexuelle des enfants en ligne
- mieux comprendre la menace et son évolution
- permettre une meilleure compréhension de l'impact sur les victimes mais aussi sur la société en général
- comparer les progrès avec l'évaluation mondiale de la menace 2018 afin de surveiller l'évolution de la nature et de l'étendue de la menace ainsi que l'impact positif des interventions
- fournir des études de cas récentes pour permettre aux membres d'établir des priorités lorsqu'il s'agit de prendre des décisions d'investissements individuelles et collectives et d'intervenir.

Méthodologie

Ce rapport est une méta-étude qui associe les résultats de plusieurs études internationales pour en augmenter l'impact et la puissance, disposer de meilleures estimations sur l'étendue de l'exploitation sexuelle des enfants en ligne dans le monde, et pour fournir une évaluation lorsque les différents rapports contiennent des données divergentes. Cette deuxième évaluation est appuyée par les recherches préliminaires des études de cas opérationnelles fournies par les organisations membres de WePROTECT.

Chiffres clés

18,4 millions de signalements de matériel pédopornographique ont été effectués par les entreprises technologiques américaines au NCMEC (Centre national pour les enfants disparus et exploités) en 2018.[3]

2/3 des 18,4 millions de signalements effectués au NCMEC provenaient de services de messagerie. Ces signalements risquent de disparaître si le chiffrement de bout en bout est mis en place.[4]

+ de 13,3 millions d'images douteuses traitées par le Canadian Centre for Child Protection (Centre canadien de protection de l'enfance) dans le cadre du projet Arachnid ont été signalées et envoyées aux analystes pour examen, donnant lieu à 4,6 millions d'avis de retrait envoyés aux fournisseurs.[5]

94 % du matériel pédopornographique découvert en ligne par IWF (Fondation pour la surveillance d'Internet) contient des images d'enfants âgés de 13 ans ou moins.

39 % du matériel pédopornographique découvert en ligne par IWF (Fondation pour la surveillance d'Internet) contient des images d'enfants âgés de 10 ans ou moins.[6]

46 millions d'images ou de vidéos uniques de matériel pédopornographique sont détenues dans les fichiers d'Europol.[7]

750 000 individus (estimation) cherchent à se connecter en ligne à des enfants pour des raisons sexuelles simultanément de par le monde.[8]

03 Conclusions sommaires

Les tendances indiquent un « raz-de-marée » d'exploitation sexuelle des enfants en ligne, avec un nombre grandissant de victimes et de survivants dans son sillage

L'étendue, la sévérité et la complexité de l'exploitation sexuelle des enfants en ligne augmentent plus rapidement que les capacités de lutte, et les signalements des partenaires de l'industrie et des services de répression ont atteint des chiffres records.[9] Par conséquent, il est urgent que les gouvernements, les services de répression, l'industrie technologique et les organisations tertiaires travaillent ensemble pour renforcer leur réponse collective.

Dans la pratique, l'obstacle à une meilleure collaboration internationale, à un meilleur partage et à de meilleures connaissances réside dans la nature morcelée de la réponse qu'apporte chaque nation à la sécurité en ligne, au travers des politiques, des services sociaux, de la réglementation et de l'éducation.

De plus en plus de personnes ont accès aux téléphones portables et à Internet, créant ainsi une asymétrie entre le Nord et le Sud. Toutes les nations font face au défi d'une technologie à évolution rapide, mais l'entrée dans le monde numérique n'est pas la même pour les sociétés qui ont adopté les services Internet de manière progressive tout en apprenant à protéger leurs infrastructures et leurs citoyens en ligne, et les sociétés qui ont reçu le produit fini instantanément, sans avoir eu le temps de développer et de faire progresser leurs services pédagogiques et de soutien, leurs services répressifs et leur réponse réglementaire. La chaîne de réponse est aussi solide que son maillon le plus faible. Un enquêteur d'Interpol la décrit ainsi :

> « C'est un peu la différence entre rentrer dans une piscine avec précaution, par l'extrémité la moins profonde, avec les outils et l'éducation nécessaires pour apprendre à nager, et être jeté dans le grand bain. [10] »

La disponibilité grandissante d'outils avancés d'anonymisation, de chiffrement de bout en bout et de réseaux de partage de fichiers pair à pair (ou P2P) donne aux délinquants un accès simplifié et plus sécurisé à des enfants vulnérables mais aussi à des réseaux d'individus qui partage un intérêt sexuel pour les enfants. Il semble y avoir un lien entre le nombre élevé de membres dans ces « lieux sûrs » et la marchandisation et l'industrialisation du matériel pédopornographique (la NCA, l'Agence nationale de lutte contre la criminalité au Royaume-Uni a identifié 2,88 millions de comptes enregistrés sur les dix sites les plus dangereux du Dark Web).[11]

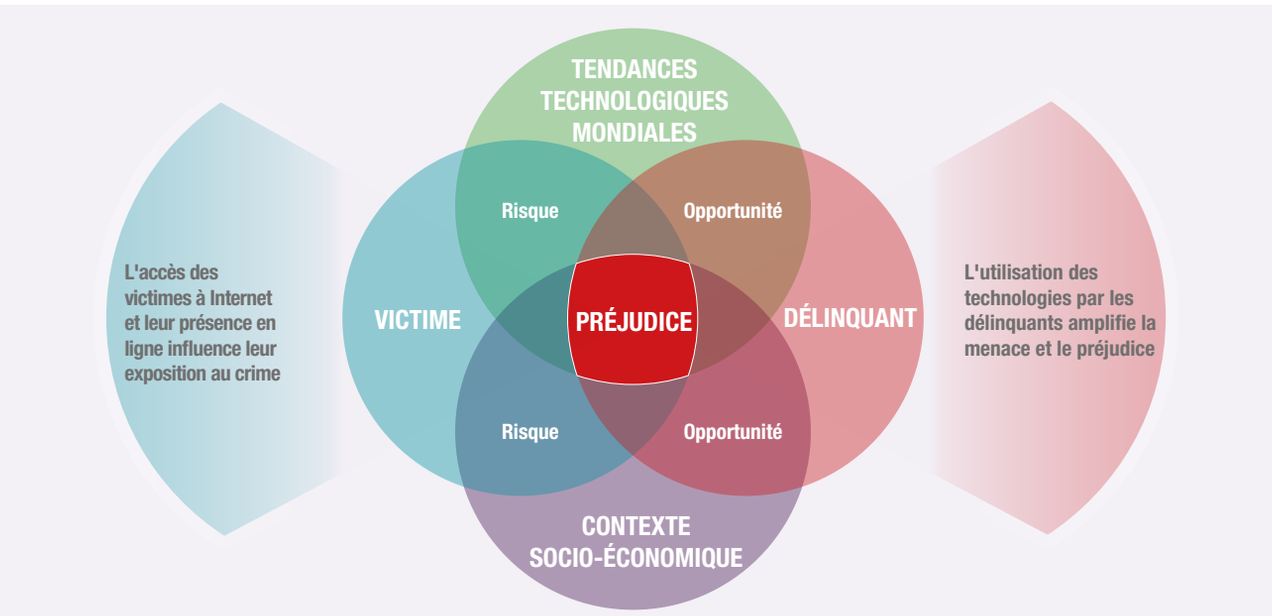
Dans le même temps, de plus en plus d'enfants possèdent un appareil et ont accès à Internet sans aucune supervision, ce qui augmente leur risque d'être exploités et abusés en ligne. Cette tendance est aggravée par leur niveau de maturité, leur compréhension limitée des risques en ligne et au changement des attitudes en ligne : un adolescent sur quatre a reçu des SMS et des e-mails explicites à caractère sexuel et un sur sept les a envoyé.[12]

Dans ce contexte, la prolifération d'images et de vidéos d'enfants indécentes en ligne est bien supérieure à la capacité des organisations chargée d'identifier et de retirer ce matériel de manière proactive. Les chapitres à venir présentent des preuves soulignant que ces menaces et ces défis sont amenés à se propager si une action décisive et commune n'est pas entreprise.

L'évaluation mondiale de la menace 2018 a identifié quatre éléments qui, associés les uns aux autres, ont le plus d'impact sur ce fléau et permettent d'expliquer l'augmentation de l'exploitation sexuelle des enfants en ligne :

- les tendances technologiques mondiales,
- le changement du comportement des délinquants,
- l'exposition en ligne des victimes,
- le contexte socio-environnemental.

Illustration 1 : Les quatre optiques du fléau : la technologie, les délinquants, les victimes et les facteurs sociaux-environnementaux.



De nouvelles recherches et études de cas à l'échelle internationale ont confirmé nos précédentes conclusions et souligné de nouveaux facteurs contribuant à un fléau grandissant. Ensemble, ils permettent de comparer l'expansion de l'exploitation sexuelle des enfants en ligne à un véritable raz-de-marée, avec un nombre lui aussi croissant de victimes potentielles qui ont besoin d'être protégées, et de survivants qui ont besoin d'être pris en charge.

Voici un résumé des quatre optiques de ce rapport ainsi que de l'illustration nº 1.

1. Des tendances technologiques mondiales : l'industrialisation des services sécurisés en ligne

L'évaluation mondiale de la menace 2018 a mis en évidence l'apparition de communautés de délinquants qui utilisent les services du Dark Web pour diffuser des images et des conseils pour solliciter les enfants et éviter d'être identifiés.[13] Ces comportements continuent et sont amplifiés par une accessibilité accrue aux services du Web visible, prêts à l'emploi, qui assurent une meilleure confidentialité, sécurité et anonymité. On compte dans ces services les réseaux sécurisés P2P de partage de fichiers, les services d'hébergement qui dissimulent le matériel pédopornographique sur les sites Web traditionnels et les services de paiement mobiles et de messagerie qui contournent le besoin d'inscription et d'identification.

2. Le comportement des délinquants : un cercle vicieux

Notre compréhension du parcours d'un criminel doit faire l'objet d'une plus grande quantité d'analyses et d'études académiques. Tous les délinquants ne se tournent pas vers les forums du Web ; tous les délinquants qui visualisent du matériel pédopornographique en ligne ne manipulent pas ou ne forcent pas les enfants à adopter un comportement sexuel explicite ; enfin, tous les délinquants qui recherchent un streaming en direct d'abus sexuels ne passent pas eux-même à l'acte sur un enfant. Les abus en ligne, en raison de la distance d'avec la victime, peuvent augmenter le risque de déviance de la part du délinquant. Il semblerait que les personnes rejoignant des « groupes d'intérêt spécial » sont encouragés à un seuil de violence plus élevé et sur des enfants encore plus jeunes, dans leur quête d'obtenir un certain statut au sein de cette communauté de délinquants.[14]

3. La vulnérabilité des victimes : la normalisation des comportements à risque en ligne

Les jeunes enfants sont de plus en plus vulnérables aux interactions dangereuses en ligne en raison de la réduction de l'âge auquel ils ont accès aux appareils et de l'accès non contrôlé aux réseaux sociaux et aux jeux en ligne. La normalisation des comportements sexuels en ligne est une tendance inquiétante. Un très grand nombre d'enfants (de plus en jeunes également) partagent des images personnelles indécentes qu'ils ont eux-mêmes prises, par tromperie ou sous la contrainte, dans le cadre d'activités consensuelles avec des enfants du même âge ou pour s'affirmer socialement. Cela met à disposition des délinquants une plus grande quantité de matériel tout en augmentant la vulnérabilité des enfants à l'exploitation et aux abus de la part des adultes ainsi que le risque d'intimidation en ligne par d'autres enfants. Certains cas montrent que les délinquants ou les fraudeurs organisés ciblent les enfants pour obtenir des images et des vidéos à caractère sexuel ; d'autres indiquent que les délinquants physiques partagent du matériel pédopornographique plus rapidement et sur une plus grande échelle que par le passé.[15]

4. Le contexte socio-environnemental : la parité technologique à tout prix

En 2018, il a y eu 367 millions de nouveaux utilisateurs sur Internet dans le monde dont Interpol estime que 1,8 million utilisateurs de sexe masculin s'intéressent aux enfants de manière sexuelle (cela ne signifie pas qu'ils deviendront tous des délinquants sexuels).[16] L'accès au monde numérique n'est pas le même au sein des sociétés qui ont adopté les services Internet de manière progressive qu'au sein de celles qui obtiennent rapidement le même niveau technologique. En effet, ces dernières reçoivent l'intégralité des services Internet de manière instantanée, sans avoir eu le temps de faire évoluer les aspects éducatifs et d'assistance, leurs services de répression ou les actions juridiques appropriées. On remarque que depuis l'évaluation mondiale de la menace 2018, le travail et l'influence mondiale de la Commission sur le haut débit pour le développement durable sont davantage axés sur l'exploitation sexuelle des enfants en ligne.[17]

Des chiffres en hausse depuis l'évaluation mondiale de la menace 2018

367 millions	de nouveaux utilisateurs d'Internet, soit une augmentation de 9 %[18]
122 millions	d'enfants supplémentaires sont désormais en ligne, selon des estimations de l'UNICEF (1 utilisateur d'Internet sur 3 est un enfant)[19]
augmentation de 80 %	du nombre de signalements de matériel pédopornographique au réseau mondial INHOPE de lignes téléphoniques d'assistance[20]
augmentation de 100 %	du nombre de photos d'enfants abusés sexuellement signalées par les entreprises technologiques[21]
augmentation de 33 %	d'URL contenant du matériel pédopornographique supprimé par la Fondation pour la surveillance d'Internet[22]

04 Tendances technologiques

Un accès à Internet de plus en plus répandu, de nouvelles technologies et un « chiffrement par défaut » favorisent la recrudescence des infractions

Le nombre d'utilisateurs d'appareils portables et d'Internet ne cesse d'augmenter. Il y a plus de cinq milliards d'utilisateurs uniques d'appareils portables et plus de quatre milliards d'utilisateurs d'Internet dans le monde, soit une augmentation de 2 et 9 % respectivement depuis 2018. Le nombre d'utilisateurs des réseaux sociaux est passé à 3,5 milliards, soit une augmentation de 9 %.[23]

L'augmentation de l'accès mobile à Internet permet une meilleure utilisation des jeux en ligne, des paiements sans espèces, du cybercommerce et d'Internet des Objets, des appareils de surveillance des bébés, des jouets connectés ou encore des appareils avec webcam. Ces produits sont de plus en plus bon marché et leur durée de vie s'allonge. Les appareils d'occasion sont de plus en plus accessibles aux consommateurs à faible revenu des nations en voie de développement.

Ces développements permettent aux nations du Sud d'atteindre la parité technologique avec les nations du Nord. Cependant, le Nord a bénéficié d'une évolution relativement stable des technologies nationales liées à Internet et aux appareils portables au cours des vingt dernières années. Les nations du Sud passent quant à elles rapidement d'un accès limité à des services Internet fiables et rapides et aux réseaux mobiles 4G et 5g, en contournant la nécessité d'établir une infrastructure coûteuse de téléphonie fixe et de haut débit.

L'année dernière, le nombre d'utilisateurs absolus en Inde a augmenté de 100 millions (soit 21 %). En matière de croissance liée à la taille de la population, huit des dix pays en tête étaient des pays africains. Djibouti, la Tanzanie, le Niger et l'Afghanistan ont chacun plus que doublé le nombre de leurs utilisateurs d'Internet d'une année à l'autre. De ce fait, sur les 20 pays en tête en matière de croissance Internet l'an passé, 19 se trouvent dans le Sud.[24]

Le modèle de réponse nationale WePROTECT apporte un cadre précieux à ces nations, leur permettant d'évaluer leur capacité à combattre l'exploitation sexuelle des enfants en ligne.

On estime à 1,8 million le nombre de nouveaux utilisateurs Internet de sexe masculin au cours des douze derniers mois portant un intérêt d'ordre sexuel aux enfants

Une des conséquences de la recrudescence du nombre d'appareils et de l'accès à Internet est l'augmentation en parallèle du nombre d'adultes en ligne ayant un intérêt d'ordre sexuel aux enfants, et du nombre d'enfants courant le risque d'être exposés à ces individus au cours d'interactions en ligne sans surveillance.

Illustration 2 : La croissance numérique de jan. 2018 à jan. 2019[25]

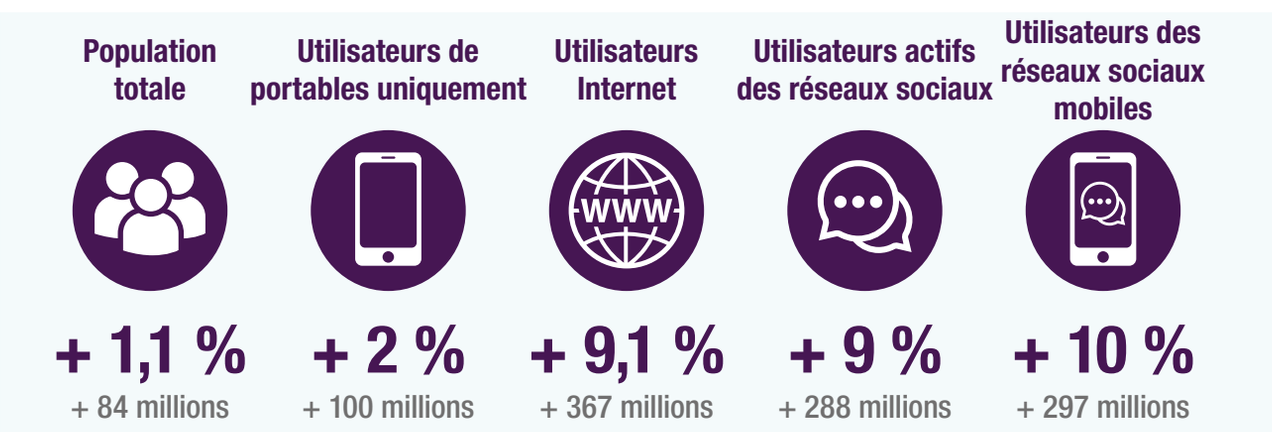
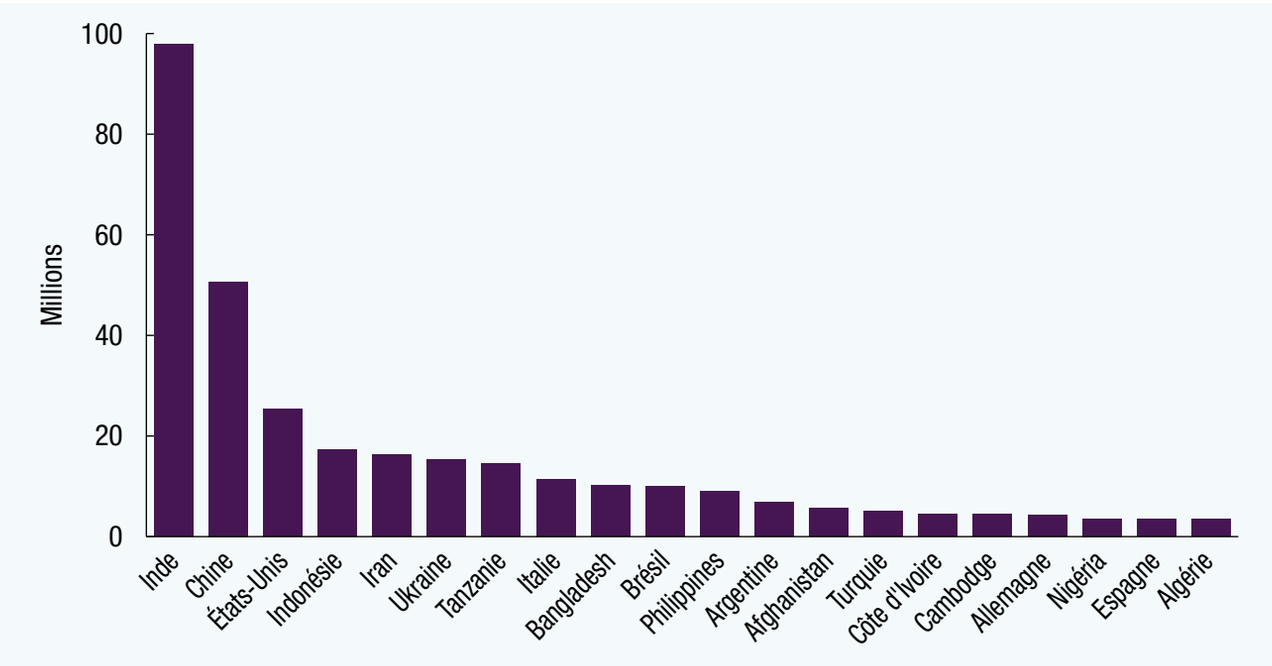


Illustration 3 : les 20 pays avec le taux le plus élevé de croissance Internet absolue (2018-2019)



Selon des estimations académiques, 1 % de la population masculine est prédisposée à un intérêt d'ordre sexuel envers les enfants prépubères. Interpol estime ainsi qu'il pourrait y avoir environ 1,8 million d'hommes supplémentaires dans cette catégorie utilisant Internet en un an (si l'on se base sur une proportion femme/homme égale).[26] Il s'agit d'une estimation prudente puisque ce 1 % fait seulement référence aux pédophiles ayant un intérêt d'ordre sexuel envers les enfants prépubères. D'autres études estiment que 2,2 à 4,4 % des hommes adultes ont sciemment visionné en ligne du matériel pédopornographique d'enfants prépubères.[27]

Une grande proportion de la recrudescence de l'accès à Internet vient du Sud. Le risque posé par ces nouveaux utilisateurs est davantage amplifié par l'absence généralisée d'éducation coordonnée sur la sécurité en ligne, par des services de police et des services sociaux moins développés. Par conséquent, un nombre supérieur d'enfants deviennent les victimes des délinquants et ne reçoivent pas l'assistance et la protection nécessaires.

La technologie favorise l'exploitation sexuelle des enfants en ligne

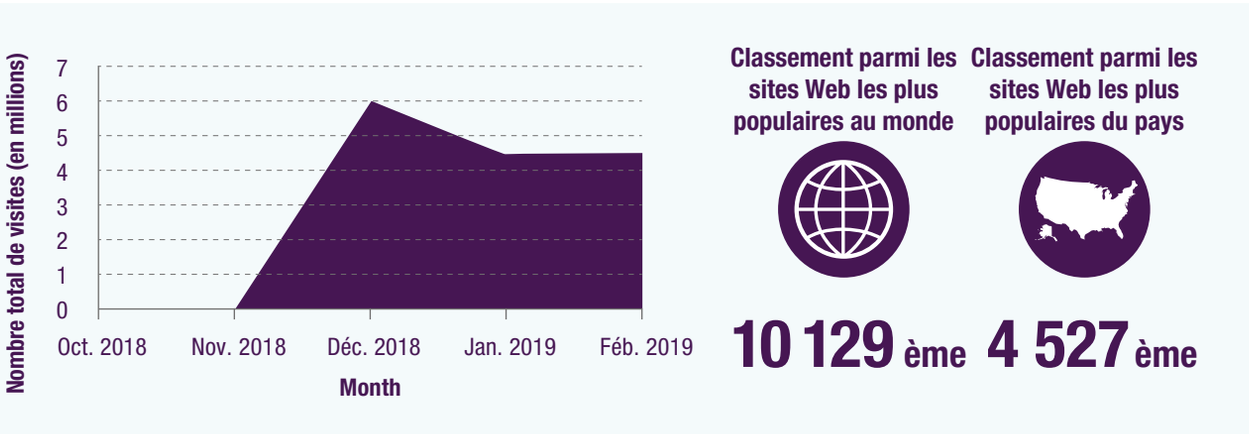
En 2018, les entreprises technologiques (ayant des utilisateurs internationaux) ont signalé plus de 45 millions de photos et de vidéos d'enfants victimes d'abus sexuels, soit le double de l'année précédente.[28]

Le niveau de disponibilité du matériel pédopornographique est considérable. Il est plus facile de créer et d'accéder aux sites web qui hébergent ce matériel pédopornographique que de les identifier et de les supprimer. Entre 2014 et 2018, le nombre d'URL liés à des abus sexuels d'enfants qui ont été supprimés a triplé par an, passant de 31 226 à 105 047 en 2018. Entre 1996 et 2019, Internet Watch Foundation (Fondation pour la surveillance d'Internet au R-U) a supprimé près d'un million de pages Web montrant des abus sexuels sur des enfants.[29]

Un site contenant du matériel pédopornographique a été consulté 6,5 millions de fois lors de son premier mois d'existence

Interpol a identifié un site sur le Web visible qui a été consulté 6,5 millions de fois lors de son premier mois d'existence en novembre 2018, pour se stabiliser ensuite à 4,67 millions de visites par mois. En février 2019, il se classait à la 4 527ème place des sites Web les plus populaires aux États-Unis et à la 10 129ème place au monde.[30]

Illustration 4 : Résumé du trafic d'un site Web populaire contenant du matériel pédopornographique (février 2019)



Notre évaluation mondiale de la menace 2018 a souligné des sites Web semblables sur le Dark Web dotés d'environ un million de visiteurs.[31]

Sur le Dark Web, les délinquants peuvent rechercher du contenu plus spécifique. En 2018, 2,88 millions de comptes ont été enregistrés de par le monde sur les dix sites les plus dangereux du Dark Web en matière d'exploitation sexuelle des enfants en ligne.[32] Le Dark Web peut amplifier le comportement des délinquants : ces lieux perçus comme « sûrs » permettent aux délinquants de discuter de leurs intérêts sexuels de manière plus ouverte et de partager des images encore plus choquantes. Cependant, l'utilisation du Dark Web et du Web visible n'est pas binaire. Les autorités canadiennes ont identifié de grandes quantités de contenu crypté et stocké dans des emplacements sécurisés sur le Web visible et leurs liens partagés sur des forums du Dark Web.[33]

La montée en puissance du cryptage

Nous avons tendance à associer le Dark Web à un environnement en ligne synonyme d'anonymat, de cryptage et de sécurité contre la détection, et d'une utilisation destinées à dissimuler des activités criminelles. Nous associons normalement le Web visible à une facilité d'accès et à la disponibilité générique de services de consommation traditionnels. L'impact du chiffrement de bout en bout des réseaux sociaux et des services de messagerie traditionnels, associé à une inscription très facile et à l'utilisation de réseaux privés virtuels (ou VPN), ont créé un environnement hybride doté de fonctionnalités idéales pour les délinquants, où les utilisateurs peuvent appliquer la sécurité et l'anonymat de base du Dark Web dans leurs interactions sur le Web visible.

L'évaluation de la menace que représente la criminalité organisée sur Internet (IOCTA) d'Europol stipule que la majorité du matériel pédopornographique continue d'être partagé via des réseaux de partage de fichiers pair à pair (ou P2P).[34] Les plateformes de réseaux sociaux et de communications accessibles au public sont toujours les méthodes les plus utilisées pour rencontrer et solliciter les enfants en ligne. En 2018, Facebook Messenger était responsable de près de 12 millions des 18,4 millions de signalements de matériel pédopornographique à l'échelle mondiale.[35] Ces signalements risquent de disparaître si le chiffrement de bout en bout est mis en œuvre par défaut, puisque les outils utilisés actuellement pour identifier le matériel pédopornographique ne fonctionnent pas dans les environnements à chiffrement de bout en bout. En outre, les réseaux de partage de fichiers pair à pair (ou P2P) permettent aux criminels de se dissimuler pour accéder au matériel pédopornographique et le partager.[36]

La recrudescence du cryptage par défaut favorise davantage les infractions sur le Web visible : le public est de plus en plus sensibilisé aux risques de sécurité en ligne et souhaite davantage protéger ses communications privées, ce qui amène de nombreux fournisseurs d'email et de messagerie à se tourner vers le cryptage par défaut. Ceci permet à un plus grand nombre de délinquants, y compris ceux ne disposant pas de capacités techniques très développées, à partager du matériel pédopornographique, des conseils et des techniques de manière sécurisée et anonyme. WhatsApp, qui fournit un chiffrement de bout en bout à ses utilisateurs, était le service de messagerie le plus populaire au monde en 2018. Il était présent dans 133 pays et territoires.[37]

De plus en plus de services traditionnels passent au chiffrement de bout en bout ou fournissent des services temporaires (tels que la suppression automatique de messages et d'images), c'est la raison pour laquelle les chefs de gouvernements

incitent les leaders industriels à s'assurer que la confidentialité et la sécurité en ligne ne nous rendent pas davantage vulnérables dans le monde réel. Un débat public est toujours en cours sur la protection de la vie privée des utilisateurs et la protection des personnes, tout particulièrement les enfants et les adultes vulnérables, des criminels.

Le forum Child's Play du Dark Web

En 2017, un Américain et un Canadien ont été arrêtés pour leur gestion de deux des plus importants sites de matériel pédopornographique du Dark Web, « Child's Play » et « Giftbox ». À leur apogée, ces sites avaient plus d'un million de profils d'utilisateurs inscrits (il est possible que certains utilisateurs aient plus d'un profil chacun). Certaines publications, appartenant à la catégorie la plus sérieuse d'abus, était visionnées plus de 770 000 fois.

Suite à une enquête menée conjointement par les forces de police des États-Unis, du Canada, d'Australie et de pays européens, appuyées par une équipe opérationnelle commune de la NCA, les deux délinquants ont été arrêtés en Virginie (États-Unis) où le délinquant canadien s'était rendu pour rencontrer son « homologue » américain. Arrêtés et interrogés, les délinquants ont fourni aux services de répression les noms d'utilisateurs, les mots de passe et les clés de cryptage du site.

Avec l'autorisation des forces de police européennes, les mots de passe et les serveurs ont été dévoilés aux forces de l'ordre australiennes. Elles ont continué à gérer Child's Play en Australie, sur autorisation juridique, un enquêteur se faisant passer pour l'administrateur du site. Les preuves ainsi recueillies ont permis d'identifier et de secourir une douzaine d'enfants au Canada. Plus de 100 victimes ont été signalées à l'échelle internationale et un pays à lui tout seul a identifié près de 900 suspects.

Les deux délinquants ont chacun été condamné à 35 ans de prison pour avoir géré une entreprise d'exploitation d'enfants. Ils ont été condamnés à la détention à perpétuité en 2017 pour le viol d'un mineur.[38]

Les applications de messagerie les plus populaires au monde

WhatsApp
L'application de messagerie la plus utilisée au monde, dotée du chiffrement de bout en bout.

Facebook Messenger
L'application de messagerie de Facebook permet aux utilisateurs de partager des fichiers, leur localisation géographique et d'envoyer de l'argent dans certains marchés. Prévoit d'incorporer le chiffrement de bout en bout.

WeChat
L'application la plus populaire en Chine, avec plus d'un milliard d'utilisateurs. Permet de partager des photos et des vidéos, de passer des appels vidéo, de partager sa localisation géographique, d'effectuer des paiements numériques et de jouer. Utilise le chiffrement de transport, c'est-à-dire que les messages sont cryptés entre l'utilisateur et les serveurs WeChat.

Viber
Plus d'un milliard d'utilisateurs, la messagerie cryptée et les conversations autodestructrices sont possibles.

Line
Très populaire en Asie, avec plus de 600 millions d'utilisateurs. Appels vers les lignes fixes et appels vidéo gratuits ligne fixe vers ligne fixe et appels vidéo. Prend en charge les conversations cryptées.

Telegram
Des millions d'utilisateurs actifs et des conversations cryptées hautement sécurisées.[39]

Le chiffrement de bout en bout pose un risque pour les enfants car il empêche les plateformes en ligne et leurs modérateurs d'identifier, de supprimer et de signaler le contenu dangereux sur les parties essentielles de leurs propres réseaux. Pourtant, de nombreux fournisseurs de services semblent accélérer la mise en place du chiffrement de bout en bout et appliquer la technologie traditionnelle qui crypte également le nom du site Web requis par un criminel.[40] La technologie basée sur le protocole (également connue sous le nom de Domain Name System (DNS) sur HTTPS ou DoH) prend le nom du domaine que l'utilisateur a saisi dans son navigateur et envoie une requête au serveur DNS pour connaître l'adresse IP numérique du serveur Web qui héberge ce site. C'est également ainsi que fonctionnent les DNS normaux. Cependant, un DoH reçoit la requête et l'envoie à un serveur DNS compatible DoH (programme de résolution) par le biais d'une connexion HTTPS cryptée et non en texte simple. De cette manière, le DoH dissimule les requêtes DNS dans le trafic HTTPS normal, de sorte que les observateurs tiers ne puissent pas surveiller ni signaler les requêtes traitées par les utilisateurs et connaître ainsi les sites Internet qu'ils sont sur le point de consulter. Ceci pourrait avoir une incidence sur les mécanismes qui bloquent les adresses Web hébergeant du matériel pédopornographique et rendre les filtres Web parentaux et scolaires inefficaces. L'industrie des technologies débat toujours des avantages et des inconvénients, mais DoH a déjà été mis en œuvre sur au moins un des navigateurs de premier plan et il est prévu de le déployer « par défaut » aux États-Unis. D'autres navigateurs prévoient de faire la même chose.

Les applications du Web visible permettent aux délinquants disposant de faibles connaissance technologiques d'accéder à du matériel pédopornographique. Le Dark Web quant à lui plaît aux délinquants plus sophistiqués et aux personnes qui recherchent des moyens supplémentaires d'éviter d'être identifiées. On ne peut accéder à ces services que par l'intermédiaire de « réseaux superposés » sécurisés qui nécessitent un logiciel spécifique. Il peut s'agir de réseaux privés virtuels (VPN), de réseaux P2P et de la méthode Tor (The Onion Router) par laquelle les données d'un utilisateur sont cryptées puis transférées via plusieurs relais pour créer un cryptage doté de plusieurs couches, protégeant ainsi l'identité et la localisation géographique de l'utilisateur.[41] Le département de la Justice américain (DoJ) précise que les sites du Dark Web bénéficient de plus de 40 000 nouveaux utilisateurs par mois. Ils restent des utilisateurs pendant plusieurs années.

Les conséquences désastreuses du cryptage sur les enfants

L'an dernier, les autorités de police européennes ont reçu plus de 600 000 signalements de cas d'exploitation sexuelle des enfants en ligne.

Le sauvetage d'une petite fille de neuf ans abusée par son père pendant plus d'un an et celui de 11 enfants exploités par un réseau, sont deux exemples parmi tant d'autres des affaires traitées au quotidien par les services de répression de l'UE.

Le commissaire européen en charge des affaires intérieures a souligné les conséquences désastreuses pour les enfants du cryptage des applications de messagerie du fait que les services de répression ne reçoivent plus les signalements dont ils bénéficient aujourd'hui.[42]

Parallèlement à l'adoption croissante d'Internet dans le Sud, on a assisté à une utilisation croissante de ces techniques. Les sites du projet Tor indiquent que les utilisateurs des États-Unis, de Russie, d'Allemagne, de France, du Royaume-Uni, d'Ukraine et des Pays-Bas constituent un peu plus de la moitié (environ 55 %) des utilisateurs de Tor. Toutefois, au cours des deux dernières années, la part des utilisateurs d'Iran, d'Indonésie et d'Inde a augmenté de 14 %.[43] Il convient de noter que ces chiffres ont trait à la croissance de Tor dans son ensemble et peuvent inclure des inscriptions à des fins légitimes et illégitimes, y compris pour les droits de l'homme et la liberté d'expression.

Se fondre dans la masse

Les délinquants recherchent constamment de nouveaux moyens de partager du matériel pédopornographique sans être identifiés par les services de répression, par exemple par le biais de sites Web « déguisés » qui utilisent des techniques d'hébergement sophistiquées qui permettent aux sites contenant du matériel pédopornographique de se fondre dans la masse. Un site affichant des images légales à un utilisateur traditionnel (ou à un enquêteur) peut révéler du matériel pédopornographique à un utilisateur qui a visité certains sites dans un ordre bien précis avant de consulter ce site en question. Une chaîne de cookies fonctionne comme une clé qui déverrouille un contenu masqué une fois que le délinquant a terminé la séquence.[44]

L'expression « non-souverain » a trait à la souveraineté des données, c'est-à-dire l'idée que les données sont soumises à la législation et aux structures de gouvernance de la nation dans laquelle elles sont recueillies. Des services non-souverain s'étendent au-delà des frontières nationales et ont été spécifiquement conçus pour ne pas dépendre d'une juridiction clairement définie. Cela permet aux délinquants de produire du contenu dans une juridiction, de l'héberger dans une autre, à l'attention de consommateurs situés dans une troisième juridiction. Il est alors presque impossible pour les gouvernements nationaux et les services de répression d'émettre des mandats ou des avis nationaux sans la présence d'une coopération internationale sophistiquée.

Des applications non-souveraines

Le département de la Justice américain (DoJ) essaie d'identifier et de protéger un mineur qu'un groupe de délinquants force à produire des images personnelles indécentes par le biais d'une application populaire de réseaux sociaux et de messagerie.

De par sa conception, cette application est non-souveraine et l'entreprise promeut le fait qu'elle n'a jamais fourni aucune information à un gouvernement. Le département de la Justice américain a essayé de prendre contact avec l'entreprise par plusieurs moyens, ne cherchant qu'à obtenir les informations propres à l'utilisateur dans le but d'identifier la victime.

Toutes les tentatives sont restées vaines et l'assignation a été renvoyée à l'envoyeur.[45]

Un autre défi auquel sont confrontés les services de répression est l'utilisation de réseaux de diffusion de contenu (CDN) ou de « services de relais » qui copient les pages d'un site Web vers un réseau de serveurs qui sont répartis dans plusieurs emplacements géographiques. Lorsqu'un utilisateur demande une page Web qui fait partie d'un CDN, celui-ci redirige la requête du serveur du site d'origine vers un serveur situé dans le CDN le plus proche de l'utilisateur et accède à la demande. Ce processus de passage d'un CDN à un autre est invisible pour l'utilisateur. Pour qu'un utilisateur se rende compte qu'un CDN a été consulté, il faudrait que l'adresse URL fournie soit différente de l'URL qui a été demandée.

De nouvelles infractions favorisées par la technologie

Le matériel pédopornographique est partagé de nombreuses façons, qui étaient ou non largement disponibles il y a quelques années. Citons par exemple le streaming en direct d'abus, les abus sur commande et les images personnelles indécentes créées par les victimes elles-mêmes, ainsi que la présence de contenu sur des systèmes de registre distribué. L'avènement du cryptage, de la réalité alternative/mélangée/virtuelle/augmentée et la décentralisation du Web ont déjà des conséquences sur la production de matériel pédopornographique et sur la manière dont il est diffusé et consommé.

En 2018, deux pour cents des plaintes reçues sur la ligne d'assistance téléphone INHOPE en République d'Irlande concernait des images virtuelles d'abus sexuels sur des enfants. [46] Des chercheurs allemands ont identifié 274 liens vers du contenu d'abus sexuels sur des enfants dans la blockchain Bitcoin.[47]

La technologie facilite davantage le streaming en direct d'abus physiques « dans la pièce » à l'échelle internationale, la plupart d'entre eux ayant lieu aux Philippines.[48] Dans les nations du Sud, où le niveau de pauvreté et le nombre d'enfants vulnérables sont élevés, les risques associés à l'adoption rapide d'une connexion Internet haut débit combinée à la disponibilité d'appareils connectés relativement bon marché sont plus importants.

L'un des défis majeurs liés au streaming en direct est la difficulté à détecter et contrôler l'acte au moment même où il se produit. Cela est dû à la difficulté d'intercepter le contenu de communications privées cryptées lorsque les canaux traversent les frontières nationales, mais aussi à la réticence d'autoriser une intrusion non ciblée, du point de vue de la vie privée et des libertés civiques. Cela s'est traduit par une demande grandissante, de la part des fournisseurs de services et des gouvernements, de mieux réguler les services qui favorisent le streaming en direct de contenu illégal.

La meilleure occasion d'identifier les délinquants et de protéger les victimes est lorsqu'un délinquant négocie l'accès à un enfant vulnérable (c'est-à-dire lorsqu'il approche et met en place la transaction avec les familles et les individus qui organisent ce type d'abus) et lorsque les images ou les enregistrements sont réalisés puis partagées sur des portails et des forums en ligne.

Un streaming en direct d'abus aux quatre coins du monde

Une enquête menée conjointement par les services de répression en Australie, en Allemagne, aux Philippines et aux États-Unis a permis l'arrestation d'un certain nombre de délinquants impliqués dans la production et la distribution de matériel pédopornographique. Un délinquant australien dirigeait un streaming en direct dans lequel une femme abusait d'enfants. La mère des enfants abusait sexuellement ses trois filles sur le Web depuis plusieurs années. Elle recevait et percevait des transferts d'argent de la part des spectateurs dans des agences locales de transferts de fonds en utilisant deux identités différentes.

Après avoir été sauvée par les services de répression, une des mineures a identifié la photo d'un autre délinquant en ligne australien, ce qui a donné lieu à un signalement aux autorités australiennes et à l'arrestation des délinquants en Australie et en Allemagne. Chaque nouvelle enquête ouverte a donné de nouvelles pistes et un circuit de signalement s'est développé de l'Australie vers les Philippines, des Philippines vers l'Australie et des Philippines vers l'Allemagne. Ce circuit continue de générer de nouvelles pistes. Ceci démontre l'importance du cycle « enquête-signalement-enquête » et les avantages de partager des renseignements avec les services de répression des autres pays.[49]

Les systèmes de paiement mobiles contournent le besoin d'inscription et de vérification de l'identité

Les techniques de paiement assistées par la technologie pour accéder au matériel pédopornographique continuent d'évoluer. Alors que des coalitions financières ont mené des interventions réussies qui ont réduit le nombre d'images payées par carte bancaire/de crédit, les services de paiement en ligne et de transfert d'argent et les centres locaux de paiement sont maintenant fréquemment utilisés.

Une méthode de paiement populaire est le système informel de transfert de valeurs (ou IVTS) qui utilise des téléphones portables sans avoir besoin de carte de crédit ni de compte bancaire. Pour recevoir l'argent, il suffit de disposer d'un numéro de téléphone portable et d'un numéro de référence. L'utilisateur n'a plus besoin de s'inscrire ni de s'identifier.[50] Les délinquants sont parmi les premiers à adopter les technologies de pointe comme les cryptomonnaies, pour pouvoir accéder discrètement au matériel pédopornographique et le partager. En juillet 2018, les forces de police bulgares ont arrêté huit personnes suspectées de disséminer du matériel pédopornographique. Les criminels utilisaient des bitcoins pour payer l'hébergement d'un site Web créé dans le simple but de transférer des images et des vidéos d'abus sexuels sur des enfants.[51]

Plus récemment, les services de répression ont assisté à une recrudescence des places de marchés en ligne qui hébergent et négocient du matériel pédopornographique sur le Dark Web. Pour y accéder, les utilisateurs doivent s'acquitter d'une somme d'argent ou fournir du matériel pédopornographique nouveau.[52]

La technologie facilite la perpétration d'un crime, mais fait également partie de la solution

La technologie ne sert pas qu'à favoriser la recrudescence du matériel pédopornographique. Elle permet aussi aux services de répression, à l'industrie des technologies et aux organisations du secteur tertiaire d'identifier, de signaler et d'empêcher le matériel pédopornographique mais aussi d'identifier et de localiser les victimes et les délinquants.

Des techniques d'enquête innovantes comme l'intelligence artificielle (IA), le suivi, la prévention des sites Web et le blocage d'images peuvent tous être déployés pour protéger les enfants en ligne. Par exemple, la campagne Localiser un objet d'Europol lancée en mai 2017 utilise les connaissances de masse pour identifier des objets capturés en arrière-plan d'une image pédopornographique.[53] Retrouver une victime grâce à sa photographie relève du défi. Cependant, le matériel pédopornographique contient souvent des objets identifiables en arrière-plan, comme des produits de la vie courante, des meubles, des bâtiments facilement reconnaissables, etc. qui peuvent s'avérer très utiles pour réduire le champ des recherches et identifier l'endroit où les abus ont lieu et protéger la victime.

L'avis des États-Unis, du Canada, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande

Au cours d'une réunion cette année, des ministres d'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis étaient tous d'avis que les sociétés technologiques ne doivent pas développer des systèmes et des services qui permettent de renforcer les capacités des criminels ou mettent en danger les personnes vulnérables. Elles doivent plutôt mettre l'accent sur la protection de leurs utilisateurs et du grand public lorsqu'elles conçoivent leurs services.

Les participants étaient tous d'avis que pour combattre le fléau que représente l'exploitation sexuelle des enfants en ligne, la réponse mondiale doit être rapidement améliorée pour faire en sorte que tous les enfants, où qu'ils se trouvent dans le monde, soient protégés et qu'il n'y ait pas de lieu sûr en ligne pour les délinquants.[54]

05 Le changement du comportement des délinquants

La technologie toujours plus sophistiquée augmente le nombre des abus et rend les enquêtes difficiles à mener

De par le monde, les causes et les origines des comportements liés aux abus sexuels sont toujours mal connues et la plupart des recherches menées sur le sujet émane du Nord. Nous comprenons beaucoup moins le parcours infractionnel de ceux qui ont un intérêt à caractère sexuel envers les enfants que les dommages en ligne causés par la distribution de contenu en ligne lié au terrorisme et à l'extrémisme.

De nombreuses années de recherche ont permis aux psychologues de déterminer comment les personnes vulnérables sont radicalisées avec des idéologies extrémistes ainsi que les étapes qui permettent d'empêcher une intensification et qui encouragent les personnes radicalisées à résister et à se désengager. On ne sait pas encore si des techniques équivalentes peuvent être adaptées pour dissuader les individus de commettre leur première infraction d'abus sexuels d'enfants, de visualiser du matériel pédopornographique et d'inciter ou d'abuser sexuellement en personne d'enfants.

Une étude portant plus généralement sur les infractions sexuelles commises par les adultes, préparée par SMART, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (le Bureau des condamnations, de la surveillance, de l'arrestation, de l'inscription et du suivi des délinquants sexuels aux États-Unis) a conclu que le problème des infractions sexuelles est trop complexe pour n'être attribué qu'à une seule théorie.[55] Un ensemble de théories offrent un meilleur aperçu des causes des infractions sexuelles.

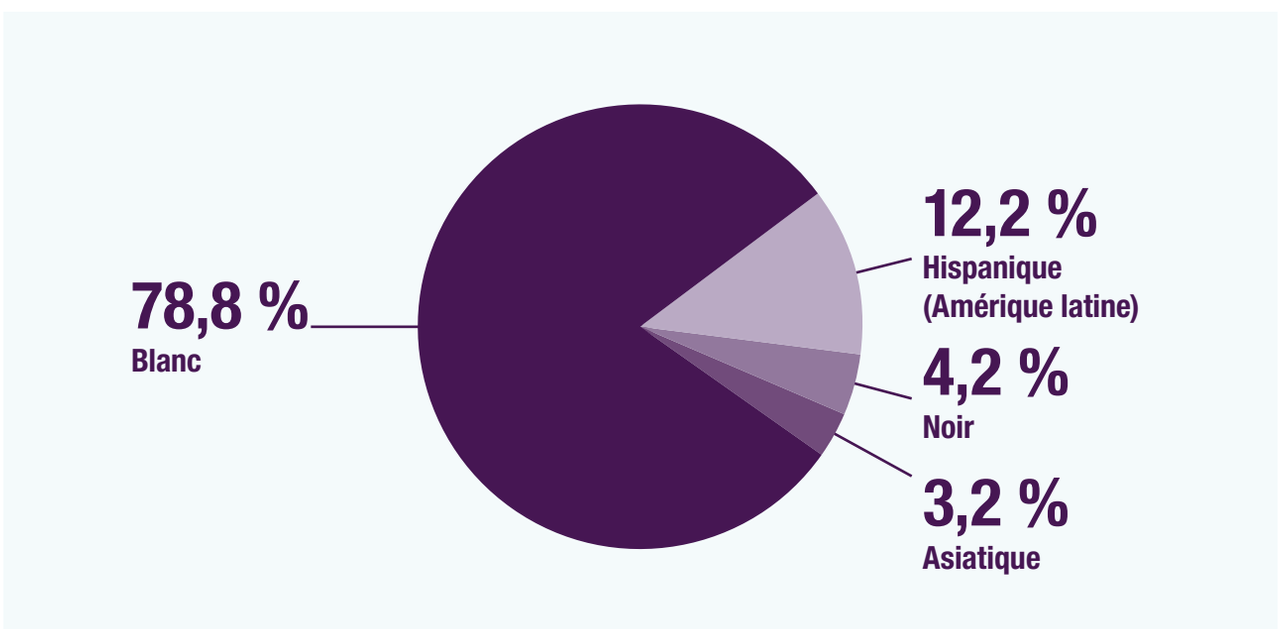
Ce que nous savons :

- Toutes les personnes ayant un intérêt d'ordre sexuel aux enfants ne commettent pas d'infractions (en sachant que les abus sexuels commis en personne, forcer à la production d'activité sexuelle en ligne et visionner des images en lignes sont toutes des infractions).
- Tous les délinquants ne sont pas des pédophiles (une orientation sexuelle chez les adultes et les personnes en fin d'adolescence qui dirigent leurs émotions ou leurs désirs sexuels ou érotiques sur les enfants prépubères). Les hébéphiles font preuve d'attirance sexuelle adulte envers les enfants pubères. Ces deux catégories doivent être différenciées de ceux présentant des troubles pédophiles ou hébéphiles, qui sont violents sexuellement envers les enfants.
- Des conditions négatives ou défavorables dans la petite enfance, en particulier de mauvaises relations avec l'autorité parentale, peuvent constituer un facteur contributif de ce comportement.

Le nombre de cas d'exploitation sexuelle des enfants en ligne est en augmentation et ceci est dû en partie aux méthodes de plus en plus sophistiquées dont disposent les nations et les fournisseurs de services Internet pour identifier et supprimer le matériel pédopornographique et combattre les délinquants. Cela permet de mieux comprendre le profil du délinquant.

L'évaluation mondiale de la menace 2018 a conclu que les délinquants ont des âges, des origines raciales, des métiers et un statut socioéconomique variés. Il s'agit d'hommes et de femmes et leur position géographique est, elle aussi, variée. Des analyses ultérieures des données de la base de données internationale sur l'exploitation sexuelle des enfants (ICSE) d'Interpol indique que 92,7 % des délinquants sont des hommes. Les délinquants de sexe féminin sont le plus souvent accompagnées d'un délinquant de sexe masculin. Les victimes ont pour la plupart la même appartenance ethnique que leur agresseur. La majorité (78,8 %) des délinquants sont blancs (à savoir qu'il est impossible de déterminer l'appartenance ethnique des délinquants dans plus de 75 % des cas et il est possible que le faible pourcentage de certaines origines ethniques soit dû au fait que la base de données ICSE ne couvre pas encore tous les pays).[56]

Illustration 5 : L'appartenance ethnique des délinquants visibles[57]



Les recherches menées conjointement par Interpol et ECPAT sur les victimes non identifiées dans le matériel pédopornographique préconisent le développement de cadres détaillés permettant une classification plus fiable des caractéristiques des victimes et des délinquants, comme l'appartenance ethnique, dans les pays et les régions du monde.

Nous assistons également à des abus commis par une génération de délinquants plus jeunes. Ils ont grandi avec les technologies et sont par conséquent plus à l'aise avec les technologies de l'information. Cette génération de criminels est donc plus à même d'identifier et d'exploiter les techniques et les services de sécurité de pointe leur permettant de ne pas être détectés.

Dans le Queensland, en Australie, une étude publiée en 2018 indique que près de la moitié des 3 035 délinquants pris en charge par le système pénal en matière de matériel pédopornographique étaient eux-mêmes des enfants de moins de 17 ans. Le nombre

de jeunes délinquants mis en garde pour possession d'images personnelles indécentes qu'ils ont eux-mêmes prises a été multiplié plus de dix fois entre 2006 et 2016.[58]

De plus, cette génération est plus moins susceptible de signaler des images d'enfants à caractère sexuel. Une campagne récente du IWF intitulée #SoSockingSimple a mis en évidence l'ignorance et le manque de connaissances chez les jeunes hommes adultes, qui ignorent que le visionnage de matériel pédopornographique est illégal et doit être signalé.[59]

L'évaluation stratégique nationale menée par la NCA ou National Crime Agence (l'Agence nationale de lutte contre la criminalité britannique) en 2019 indique que l'exploitation sexuelle des enfants en ligne est une gratification sexuelle. D'autres individus cherchent à profiter financièrement en vendant en ligne du matériel pédopornographique (surtout des abus diffusés en direct) ou en monétisant le trafic Internet lié à du matériel pédopornographique grâce à la publicité « au coût par click ».[60] Les abus diffusés en direct à des fins commerciales sont une menace grandissante. En effet, pour une somme aussi modique que 10 à 20 euros, les délinquants peuvent organiser les abus, en temps réel, sur l'enfant de leur choix.[61] Pour certains, le matériel pédopornographique est une forme de monnaie dans les réseaux d'abus d'enfants. Les agresseurs utilisent le matériel pour obtenir plus de notoriété ou pour acheter/vendre des photos et des vidéos jamais visionnées.

La plupart des délinquants demeurent des personnes très effacées qui agissent tous seuls. Cependant, la création de « lieux sûrs » numériques engendre un regroupement des délinquants dans les forums et les plateformes en ligne des fournisseurs de services du Dark Web, qui bénéficient de la messagerie cryptée et de streaming. Les délinquants n'y font pas que du visionnage d'images. Ils ciblent activement les enfants aux quatre coins du monde via des plateformes commerciales pour les manipuler et les forcer à leur fournir des images explicites ou pour les rencontrer en personne.

De plus, l'accès généralisé au matériel pédopornographique sur le Web visible favorise la perpétration d'abus. Ce type de communautés normalise le comportement des délinquants, les encourage et valide leur comportement et leur permet de partager le matériel/leur expérience et d'accroître leurs connaissances. Ils sont donc moins susceptibles de demander de l'aide et leurs chances de commettre des abus sont ainsi plus élevées. Le manque de dissuasion et de services de soutien joue peut-être également un rôle car certains individus ayant un intérêt d'ordre sexuel envers les enfants peuvent ne pas savoir vers qui se tourner pour obtenir de l'aide, le cas échéant.

Une aggravation potentielle

Le droit fait normalement la différence entre les individus qui amassent du matériel pédopornographique pour leur utilisation personnelle et ceux qui en amassent et le partagent activement d'une part, et les individus qui commettent les abus en personne et ceux dont les abus d'enfants sont commis exclusivement en ligne d'autre part.

Ces différences sont importantes car elles indiquent une aggravation potentielle, avec d'un côté ceux qui recherchent et visualisent des images existantes et ceux qui manipulent ou forcent des enfants à se soumettre à des activités sexuelles explicites via leurs propres webcams (y compris des attouchements sur leur propre personne ou entre deux victimes) et de l'autre, des individus qui paient pour diriger et observer les abus en train d'être commis par un agresseur dans la même pièce, à ceux commettant les abus en personne.

Cependant, cette aggravation n'est pas une fatalité. Il existe de nombreuses opportunités d'empêcher ou de dissuader ces individus qu'Europol décrit comme de « simples spectateurs », permettant ainsi aux services de répression de concentrer leur attention sur les délinquants les dangereux et les plus aguerris. Selon l'UNICEF, la plupart des délinquants en ligne n'ayant jamais commis d'abus sexuels en personne ont peu de chance de commettre des abus sexuels en personne un à cinq ans après avoir commis leur première infraction.[62] Cependant, tout porte à croire que les abus en ligne ouvrent la porte des risques plus grands de déviance car le comportement du délinquant est moins entravé par la peur de la détection ou de l'identification.[63]

Évolution du parcours des délinquants

Un certain nombre d'affaires traitées par la NCA indiquent à quel point les technologies modifient la façon dont certains délinquants commettent les abus, la dépravité des abus et le parcours des délinquants lui-même.

Dans une affaire, un délinquant a rejoint un groupe de discussion privé en ligne destiné aux individus ayant un intérêt d'ordre sexuel pour les enfants. Les nouveaux membres devaient poster de nouvelles images d'abus et le délinquant a ainsi violé une petite fille de six mois, abusé sexuellement d'un garçon de deux ans, diffusé les vidéos sur une application cryptée et partagé ces vidéos sur un site de partage de fichiers populaire.[64]

Dans une autre affaire, un délinquant a envoyé de l'argent à des individus connus pour organiser des abus sexuels sur des enfants diffusés en direct aux Philippines. Il a été arrêté dès son retour au Royaume-Uni. Les analyses médico-légales ont montré que ce délinquant avaient effectué au moins 15 transferts d'argent vers de tels individus entre août 2017 et juin 2018 et des images d'abus d'enfants ont été retrouvées sur son téléphone.[65]

Un autre délinquant a été condamné en février 2018 à 25 ans de prison après avoir plaidé coupable de 137 infractions de sadisme absolu sur 300 victimes sur le Dark Web. Le délinquant a eu accès à des enfants en ligne en les forçant et en leur faisant du chantage sur des forums ouverts et des sites de commerce en ligne. Les conversations sont ensuite passées sur des plateformes sécurisées et cryptées où il les a forcé à effectuer des activités sexuelles et les a soumis à du chantage. Le délinquant a forcé les victimes à des activités de plus en plus dépravées en les menaçant de distribuer des images d'abus et leurs renseignements personnels sur le Dark Web. [66,67]

Ces affaires montrent l'aggravation et l'incitation au travers du réseautage avec d'autres délinquants sur le Web visible et sur le Dark Web, où les discussions avec des individus partageant les mêmes intérêts conduisent souvent les délinquants à partager leurs méthodes pour perpétrer les abus et éviter la détection.

Ensemble, ces trois études de case indiquent une évolution du parcours des délinquants et établissent une relation claire entre les abus indirects et les abus en personne.

Certains délinquants, arrêtés pour visionnage ou possession d'images indécentes d'enfants, affirment qu'ils n'ont commis aucune infraction puisqu'il n'y a eu d'abus en personne et qu'ils n'ont contraint personne surtout lorsque ce sont les enfants eux-mêmes qui ont mis en ligne les images et les vidéos. Dans 150 des 195 pays couverts par le projet « État de droit » de l'ICMEC ou International Center for Missing and Exploited Children (Centre international des enfants disparus et exploités), la législation nationale répond désormais au critère 4, selon lequel posséder sciemment du matériel pédopornographique avec ou non l'intention de la distribuer, est un crime.[68]

D'un point de vue de la protection, faire la différence entre des abus en personne et des abus sans contact est trompeur. Lorsque les délinquants ne se trouvent pas physiquement dans la même pièce mais dirigent les abus à distance, les victimes de ces abus par attouchements sur leur propre personne risquent de se sentir encore plus coupables et honteuses, ce qui peut rendre leur rétablissement plus difficile.[69]

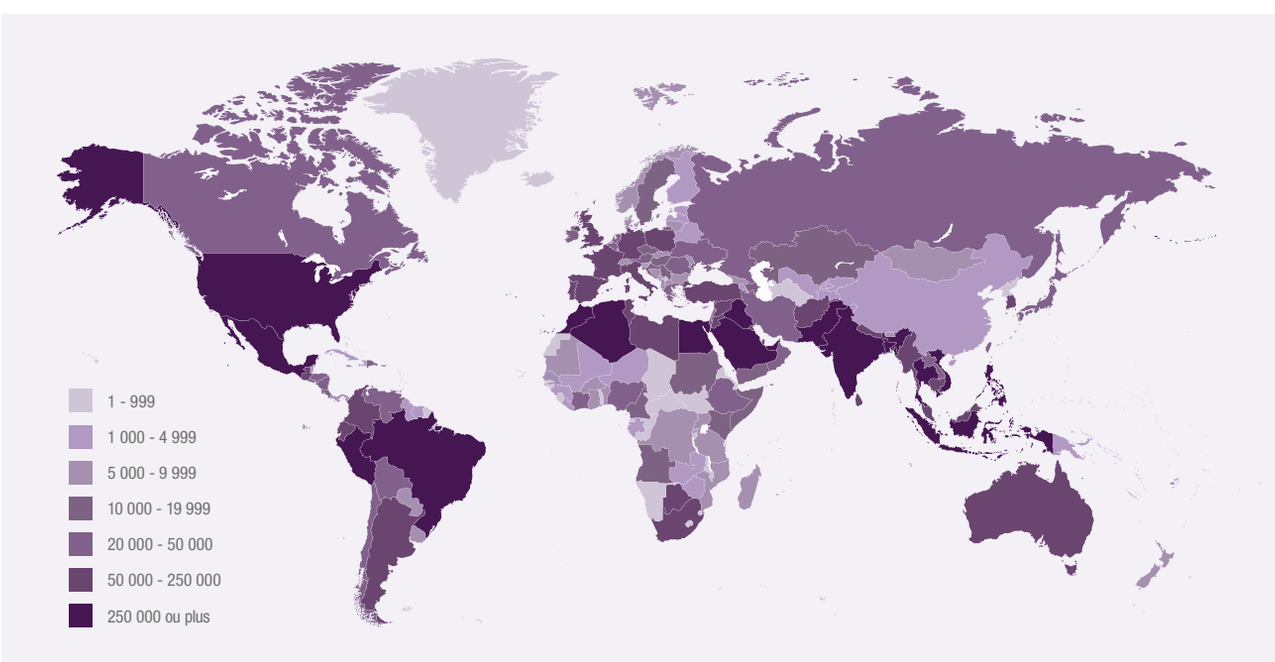
Les données démographiques des délinquants sont à l'image de leurs communautés

Une étude menée par le CSA Centre (Centre britannique d'expertise sur les abus sexuels sur les enfants) a démontré que dans le Nord, la contribution des criminels sur le plan de l'emploi et de l'économie était cohérente avec les taux de leurs communautés.[70] Par exemple, les recherches menées par la British Association of Social Workers ou BASW (l'Association britannique des travailleurs sociaux) ont démontré que le délinquant en ligne type au Royaume-Uni était un homme blanc célibataire entre 20 et 30 ans, éduqué, salarié et sans antécédents de troubles mentaux sévères ni de problèmes sérieux dans son enfance.[71] Ceci concorde avec les données d'autres services de répression et d'organisations non-gouvernementales, qui indiquent que les hommes sont bien plus susceptibles de perpétrer l'exploitation sexuelle des enfants en ligne.

Il est possible que ce constat ne soit pas probant. En effet, une grande proportion des infractions ne sont pas signalées et les abus commis par les femmes ne sont, en grande majorité, ni détectés, ni signalés.[72] Il est possible que le profil actuel du délinquant reflète les données démographiques des nations riches, qui ont bénéficié d'une croissance rapide en matière d'adoption des technologies, d'accès aux appareils et à Internet.

Comme nous l'avons vu au chapitre 4, il n'est pas possible d'établir le lien avec précision entre les données démographiques des individus qui produisent, hébergent et utilisent le matériel pédopornographique car il est possible que ces trois activités aient lieu dans des juridictions différentes.

Illustration 6 : Signalements NCMEC 2018



La carte des signalements au NCMEC pour 2018 de la page précédente montre l'origine des plus grosses concentrations de signalements de matériel pédopornographique présumé, mettant ainsi en évidence un fléau mondial.[73]

Statistiques de l'URL IWF

87 % des URL contenant des abus sexuels d'enfants identifiés dans le monde par l'IWF sont hébergés dans cinq pays seulement : les Pays-Bas, les États-Unis, le Canada, la France et la Fédération de Russie.[74]

Des délinquants peu versés dans les technologies et des délinquants ayant une grande maîtrise des technologies

Il n'y a pas de lien direct entre l'aptitude technique et le comportant criminel. Cependant, des technologies de plus en plus sophistiquées semblent diminuer la probabilité de détection et d'arrestation et rendre la tâche des enquêteurs plus difficile.

L'évaluation mondiale de la menace 2018 a mis en évidence l'émergence de communautés de délinquants utilisant des plateformes de messagerie anonymes cryptées et hautement sécurisées qui nécessitent un niveau d'expertise technique très élevé. À cela s'ajoute une nouvelle génération de délinquants qui a vu le jour grâce à des services génériques destinés aux consommateurs dont le coût est très faible.

Les délinquants accèdent aux enfants de plusieurs façons

Des statistiques récentes publiées par les tribunaux chinois indiquent que dans environ 30 % des signalements, les victimes et les agresseurs des affaires d'abus sexuels sur des enfants entrent d'abord en contact via Internet. Cependant, les fonctionnaires des tribunaux indiquent que les « abus sexuels sur les enfants sont très peu signalés puisqu'ils ont lieu en privé » et que de nombreux cas ne passent pas en justice « pour des raisons objectives et subjectives », y compris la peur des victimes et les difficultés à obtenir des preuves.

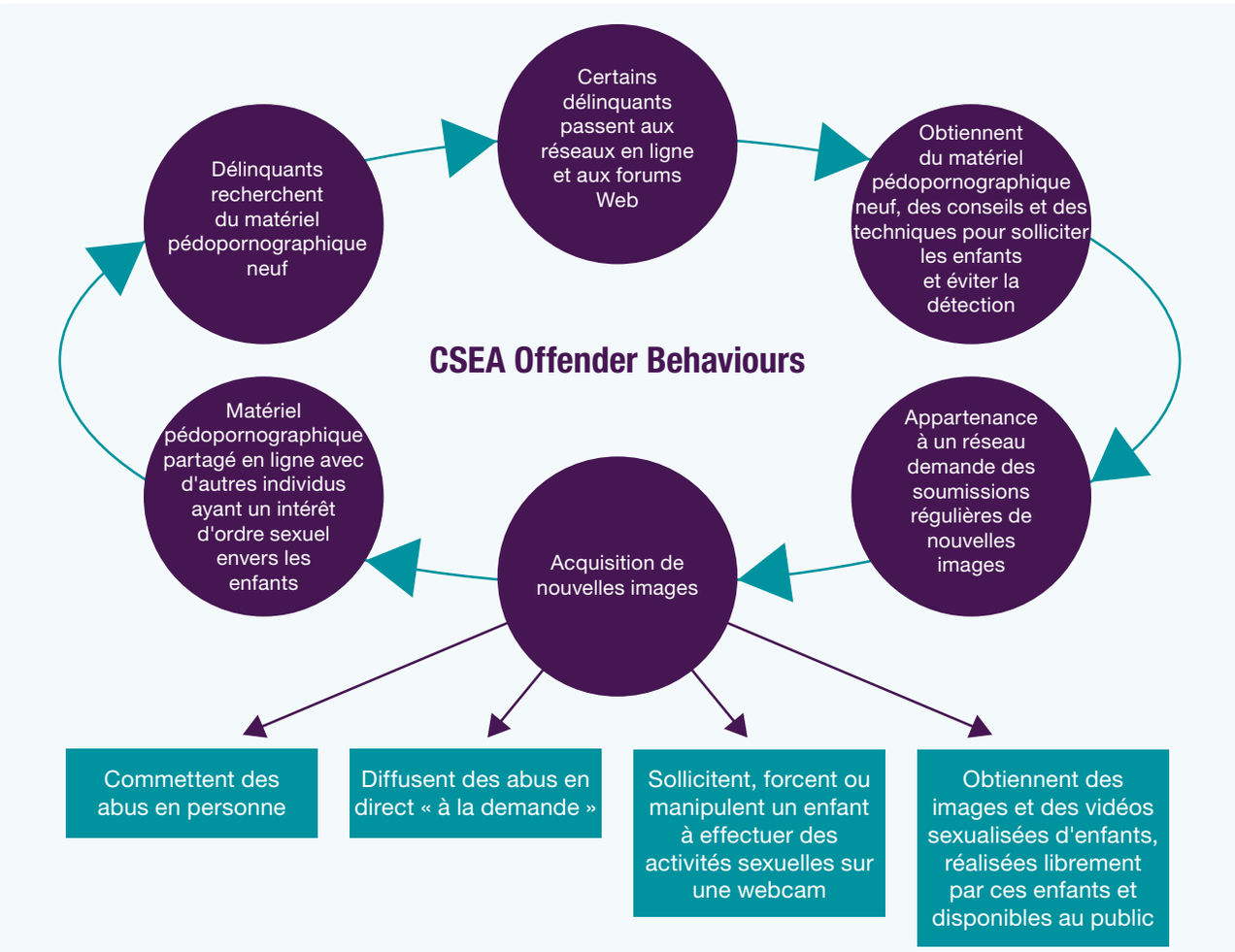
Dans une affaire, un délinquant a été condamné à 11 ans de prison pour avoir manipulé ses victimes à lui fournir des images sexuelles explicites en leur faisant croire qu'il était cadre pour une chaîne télévisée à la recherche de nouveaux talents. Le délinquant a ensuite utilisé ces images pour faire chanter ses victimes afin qu'elles lui fournissent de nouvelles photos et de nouvelles vidéos. Dans une autre affaire, un criminel de 32 ans s'est servi d'une application de rencontres pour se mettre en rapport avec des enfants, abusant une victime rencontrée via cette application dans la chambre d'un hôtel local.[75,76]

Dans une autre affaire, un délinquant d'une zone rurale de Chine a réussi à accéder aux tableaux d'affichage de Tor. Lorsqu'il s'est rendu compte que la lenteur des connexions Internet limitait ses capacités à utiliser Tor, il est passé aux sites de partage de fichiers pair à pair, utilisant souvent un VPN pour dissimuler son adresse IP.[77]

Ces études de cas montrent que les délinquants sont capables d'utiliser toute une gamme de technologies pour avoir accès à des enfants et les exploiter. Ce phénomène n'est pas propre au Nord, il est universel.

Dans le même temps, l'utilisation croissante des réseaux sociaux leur donne un accès direct et de masse aux enfants. Ceci a engendré une augmentation significative de la sollicitation, du chantage et de l'extorsion en ligne. Des délinquants solitaires peuvent cibler de nombreux enfants simultanément, et les faire chanter ou les extorquer très rapidement. En conséquence, l'exploitation sexuelle des enfants en ligne est associée à la sollicitation d'enfants sur les réseaux sociaux. Cependant, les enfants sont toujours vulnérables aux abus en personne perpétrés par des membres de leur famille et les personnes auxquelles ils font confiance. Dans certains pays, cela est souvent lié au trafic sexuel en ligne.[78, 79] 67 % du matériel pédopornographique semble avoir été réalisé dans le cadre familial.

Illustration 7 : Le comportement des délinquants vis-à-vis de l'exploitation sexuelle des enfants en ligne



Bon nombre des facteurs exposés ci-dessus engendrent un cercle vicieux de perpétration d'abus. On en retient le fait que les individus ayant un intérêt d'ordre sexuel envers les enfants recherchent de nouvelles images et vidéos indécentes en ligne, voire un contact en personne avec des enfants. Une sécurité et un anonymat accrus poussent de plus en plus ces individus vers les réseaux en ligne et les forums du Web, où ils obtiennent non seulement des images mais aussi des conseils et des techniques leur permettant de solliciter les enfants et d'échapper à la détection. Concevoir de nouvelles mesures préventives va nécessiter des recherches approfondies pour que nous puissions comprendre les causes et l'origine de ces comportements sexuellement abusifs.

06 Exposition en ligne des victimes

Des niveaux plus importants d'accès en ligne et des normes culturelles changeantes abaissent la tranche d'âge des victimes et accroissent leur vulnérabilité

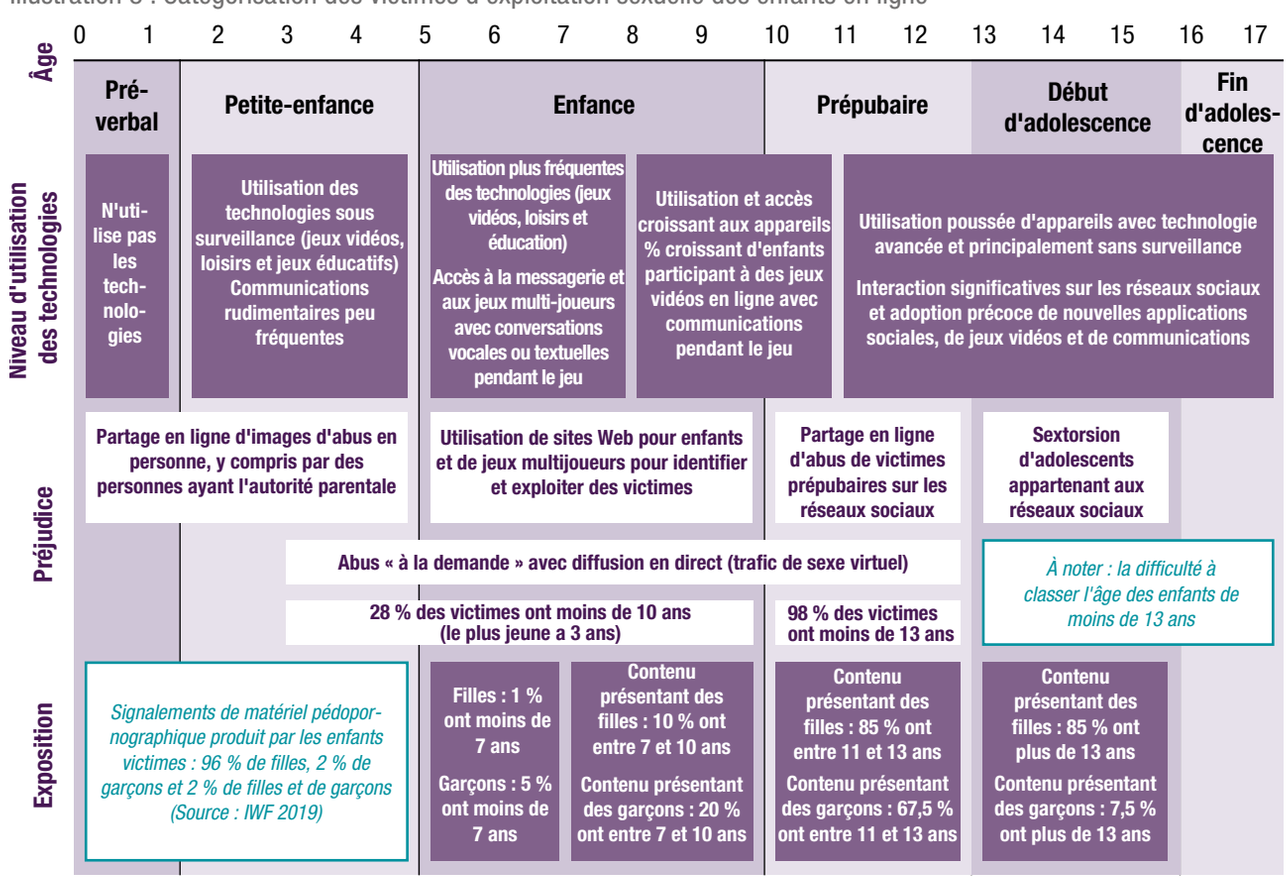
Nous avons appliqué la catégorisation des victimes suivante en fonction de leur âge et du recours à la technologie associée. Sur la base de données récentes issues d'enquêtes réalisées auprès de parents et de forums Internet consacrés à l'usage des réseaux sociaux et de services de jeux multi-joueurs par des enfants, il semblerait que l'âge moyen pour chaque type d'usage de technologie est environ deux ans plus bas que dans notre premier rapport dans le cadre du GTA18.

Quand nous catégorisons les mêmes groupes d'âge par rapport aux types de violences auxquelles ils sont exposés, et les pourcentages d'enfants dans chaque tranche d'âge qui sont exposés à différentes formes de violences, il existe une corrélation claire avec le type de technologie que chaque groupe utilise.

Selon l'UNICEF, un internaute sur trois dans le monde est un enfant.[80] Ceci correspond à 122 millions d'enfants qui ont fait leurs premiers pas en ligne pour la seule année 2018. Ceci représente un défi important pour les adultes en termes de supervision et de protection.

Des enfants deviennent propriétaires de, et/ou ont un accès non supervisé à, des dispositifs intelligents connectés à Internet à des âges plus bas, et les utilisent pour des interactions non supervisées avec des étrangers qui utilisent des réseaux sociaux et des jeux multi-joueurs en ligne.[81] Ceci expose des enfants et des personnes vulnérables à un vaste éventail de risques (le gouvernement britannique a catégorisé 29 types de violences en ligne) parmi lesquels l'exploitation sexuelle des enfants en ligne, et

Illustration 8 : Catégorisation des victimes d'exploitation sexuelle des enfants en ligne



les contenus terroristes et extrémistes en ligne tels que définis pas l'OCSE représentent le degré le plus élevé et le plus grave.[82]

Le problème est particulièrement aigu dans les sociétés prospères. De nombreux tuteurs et enseignants, qui jouent un rôle vital dans la définition des conditions de l'accès en ligne des enfants, n'ont pas fait l'expérience de ces risques et violences au cours de leur propre enfance. Par conséquent, la connaissance des dangers qui gouverne les normes d'engagement physique avec le monde extérieur ne s'est pas encore développée en ligne.

Alors que l'âge minimal recommandé pour créer un compte sur les réseaux sociaux est de 13 ans, voire plus dans certaines juridictions (et pour Facebook, Twitter, Instagram, Snapchat et d'autres sociétés de réseaux sociaux américaines, c'est un minimum légal), il existe des indications d'accès étendu à des services en ligne et la possession de dispositifs parmi les 5-13 ans et des indications claires que des enfants sont exposés au monde en ligne avant cet âge.

L'impact de l'accès non supervisé à des réseaux sociaux et les services de jeux est visible à travers le profil d'âge des sujets d'images indécentes auto-générées et les résultats des enquêtes réalisées en ligne auprès des parents et des usagers. Selon le système paneuropéen de classification par âge (PEGI), Fortnite®, un jeu multi-joueurs en ligne pour les enfants, est réservé aux plus de 12 ans, mais selon un sondage en ligne réalisé en 2018 par Survey Monkey et Common Sense Media, 26 % des parents choisissent 8-11 ans comme la tranche d'âge à laquelle les enfants devraient être autorisés à y jouer.

42 % des enfants en bas âge en Australie utilisent des dispositifs connectés à Internet à l'âge de deux ans et 81 % à l'âge de quatre ans

51 % des enfants de 6 à 13 ans en Allemagne possèdent un téléphone intelligent ou portable[83]

80 % des moins de 14 ans à Singapour ont eu accès à Internet[84]

90 % des 11-16 ans au Royaume-Uni déclarent avoir un compte sur les réseaux sociaux et 44 % des 5-15 ans possèdent un téléphone intelligent[85]

Usage émergent des plateformes de jeux

Une technique que les délinquants utilisent est d'offrir un équipement à un enfant ou une monnaie utilisable dans un jeu dont l'enfant a besoin ou qu'il désire pour un jeu particulier. Un délinquant a mentionné avoir vu une jeune fille diffuser en direct sur YouTube. Il lui a demandé si elle aimait un certain jeu et si elle voulait de la monnaie utilisable dans ce jeu. Lorsqu'elle a répondu par l'affirmative, le délinquant lui a demandé son identifiant de jeu et a commencé à discuter avec elle sur la plateforme et a fini par recevoir des images indécentes auto-générées en échange de monnaie utilisable dans le jeu.[86]

Facteurs socio-économiques

La vulnérabilité des enfants en ligne est amplifiée par une variété de facteurs socio-économiques et culturels. Des enfants deviennent propriétaires de, et/ou ont un accès non supervisé à, des dispositifs intelligents connectés à Internet à des âges plus bas, et les utilisent pour des interactions non supervisées avec des étrangers par l'intermédiaire des réseaux sociaux et des jeux multi-joueurs en ligne. Ceci expose des enfants et des personnes vulnérables à un large éventail de risques, parmi lesquels l'exploitation sexuelle des enfants en ligne et les contenus terroristes et extrémistes en ligne représentent le degré le plus élevé et le plus grave. Ce problème est particulièrement aigu dans les sociétés prospères. De nombreux tuteurs et enseignants, qui jouent un rôle vital dans la définition des conditions de l'accès en ligne des enfants, n'ont pas fait l'expérience de ces risques et violences au cours de leur propre enfance. Par conséquent, la connaissance des dangers qui gouverne les normes d'engagement physique avec le monde extérieur ne s'est pas encore développée en ligne.

En parallèle, beaucoup d'usagers dans l'ensemble du Sud reçoivent l'ensemble des services instantanément dans la mesure ou l'infrastructure de données mobiles et des dispositifs à bas prix fournissent un accès non réglementé sans l'investissement correspondant dans l'adaptation de l'éducation, de la législation, des services sociaux et des services de répression. Ce phénomène est aggravé par des normes sociales différentes en matière de sexualité des enfants et il existe des défis particuliers dans le domaine des enquêtes et du soutien aux victimes masculines, surtout dans les sociétés qui perçoivent les garçons comme endurants et mieux à même de se protéger.[87]

L'autorité des communications au Kenya rapporte que l'usage de dispositifs portables au sein de sa population de 44 millions d'habitants se situe autour de 88 %, alors même que 42 % de la population du pays vit sous le niveau de pauvreté et que les niveaux d'inégalité y sont parmi les plus élevés en Afrique.[88] Dans de telles circonstances, les enfants des groupes aux revenus les moins importants encourent un plus grand risque d'être vendus, victimes d'abus ou de traite en ligne afin de fournir un revenu à la famille.[89]

De manière similaire, au Cambodge, des zones économiques spéciales et de libre échange ont été identifiées comme particulièrement problématiques pour l'exploitation sexuelle et la traite des enfants, dans la mesure où les opportunités économiques ont rendu ces destinations attractives pour les enfants et familles originaires de régions plus pauvres.[90]

Canada
Le projet canadien Arachnid a scanné 2 milliards de pages Web dans le monde entier pour repérer des matériels pédopornographiques depuis 2016, et a émis plus de 4,6 millions des notifications de retrait à l'intention des fournisseurs de services Internet. 85 % d'entre elles concernent des victimes qui n'ont pas été identifiées par des services de répression.[91]

Cameroun, Gambie, Kenya, Togo et Ouganda
54 % des enfants ont vu quelqu'un de leur âge dans des matériels pédopornographiques en ligne, et environ 10 % des enfants ont été approchés par le biais de contacts en ligne pour partager des images à caractère sexuel.[92]

Mexique
12 300 comptes Internet distribuaient des matériels pédopornographiques au Mexique en 2017.[93]

Royaume-Uni
21 % des filles âgées de 11 à 18 ans interrogées avaient reçu des demandes d'images ou des messages à caractère sexuel.[94]

Les communautés déplacées font face à un risque accru

Un corpus croissant d'éléments de preuve suggère que des enfants dans des communautés déplacées, y compris des réfugiés et des migrants économiques, risquent davantage d'être victimes d'exploitation sexuelle des enfants en ligne en raison de la faiblesse de l'état de droit, ainsi que de l'adoption croissante des technologies au sein des communautés dans lesquelles les capacités de protection de l'enfance sont limitées.

Au Moyen-Orient, le Haut Commissaire des Nations-Unies pour les réfugiés a rapporté des cas de jeunes réfugiés masculins syriens au Liban et en Jordanie qui avaient subi un chantage pour les forcer à se livrer à des activités sexuelles par des garçons plus âgés ou des hommes qui utilisaient des téléphones portables à la dérobée pour enregistrer des images indécentes qu'ils menaçaient de mettre en ligne.[95]

En Chine, l'instabilité des États voisins a abouti à un grand nombre de personnes déplacées, avec des communautés d'enfants particulièrement vulnérables. Des services de messagerie et des plateformes de réseaux sociaux populaires sont utilisés pour faciliter la traite sexuelle de femmes et d'enfants originaires de régions rurales.[96]

La menace de déportation, par ex. pour les migrants nord-coréens, peut aboutir à ce que les victimes soient réticentes à dénoncer les abus. Des recherches menées par l'initiative pour le futur de la Corée (Korea Future Initiative) soulignent le fait que des enfants d'à peine neuf ans apparaissent dans des streams de sexe virtuel.[97] Cette vulnérabilité est particulièrement exploitée par des sociétés d'Asie du Sud-Est plus prospères, y compris en Corée du Sud, où le rapport d'une ONG a établi que 95 % de l'exploitation commerciale des enfants étaient organisés sur Internet.[98]

Facteurs culturels

Des facteurs sociaux peuvent également influer sur la vulnérabilité à l'exploitation sexuelle et à l'abus des enfants en ligne. Les enfants des communautés lesbiennes, gay, bisexuelles et transgenres sont plus susceptibles d'explorer leur orientation sexuelle en ligne, ce qui peut accroître leur vulnérabilité au chantage et à l'exploitation, tout en diminuant la probabilité qu'ils dénoncent des abus.

Une étude des matériels pédopornographiques en ligne a établi que 80 % des victimes étaient de sexe féminin, 87 % étaient caucasiennes et 83 % des délinquants adultes visibles étaient de sexe masculins.[99] Comme le fossé technologique se comble et que l'hémisphère Sud fait ses premiers pas en ligne, nous nous attendons à ce que ces statistiques reflèteront davantage une société mondialisée et des facteurs culturels, le fossé rural/urbain, l'accès à des services de soutien et des différences sociétales plus générales.

La normalisation du comportement sexuel en ligne

Des normes culturelles changeantes en matière de partage des images et des interactions sexuelles entre adultes en ligne changent le paysage. Un grand nombre d'enfants participe à la production d'images à caractère érotique ou sexuel d'eux-mêmes, qui peuvent être partagées plus largement, ou collectées et redistribuées par ceux qui ont un intérêt sexuel pour les enfants. Au cours des six premiers mois de 2019, l'IWF a traité 22 484 signalements de matériel d'abus sexuel d'enfants auto-générés.[100]

Des recherches menées par l'université d'État de l'Arizona portant sur plus de 1 000 étudiants fréquentant sept universités américaines indiquent que les « sextos » sont désormais considérés comme un élément normal du processus de rencontre moderne et qu'ils ne sont pas associés à un comportement risqué du point de vue sexuel.[101] L'IWF a rapporté que ce comportement est imité par des enfants et commence à jouer un rôle significatif dans la vulnérabilité des victimes.[102] Des enquêteurs d'Interpol ont confirmé que ce phénomène culturel ne se limite pas à l'hémisphère Nord et qu'il a des implications complexes en termes de protection des personnes vulnérables dans les sociétés où existent de forts tabous culturels et religieux par rapport aux interactions sexuelles extra-maritales.[103]

Le plus grand défi par rapport aux images indécentes auto-générées est qu'il s'agit d'une expression fourre-tout pour un éventail de comportements où le niveau de contrôle des enfants varie ; du partage entre pairs dans le cadre de relations appropriées à l'âge, jusqu'au processus de coercition où des adultes (et certains adolescents) séduisent, manipulent ou exercent un chantage sur un enfant afin qu'il se livrent à des actes sexuels devant une webcam pour obtenir des images plus explicites et les partager en ligne avec d'autres délinquants.

Concevoir des plateformes pour l'interaction adultes/enfants

En avril 2016, deux citoyens américains ont plaidé coupables pour la production de matériel pédopornographique, et la conception et l'exploitation de deux sites Internet destinés à contraindre et à inciter des mineurs d'à peine huit ans à se livrer à des activités ouvertement sexuelles devant une webcam. Dix autres membres de ce groupe à travers les États-Unis et l'Afrique du Sud ont été inculpés et condamnés.

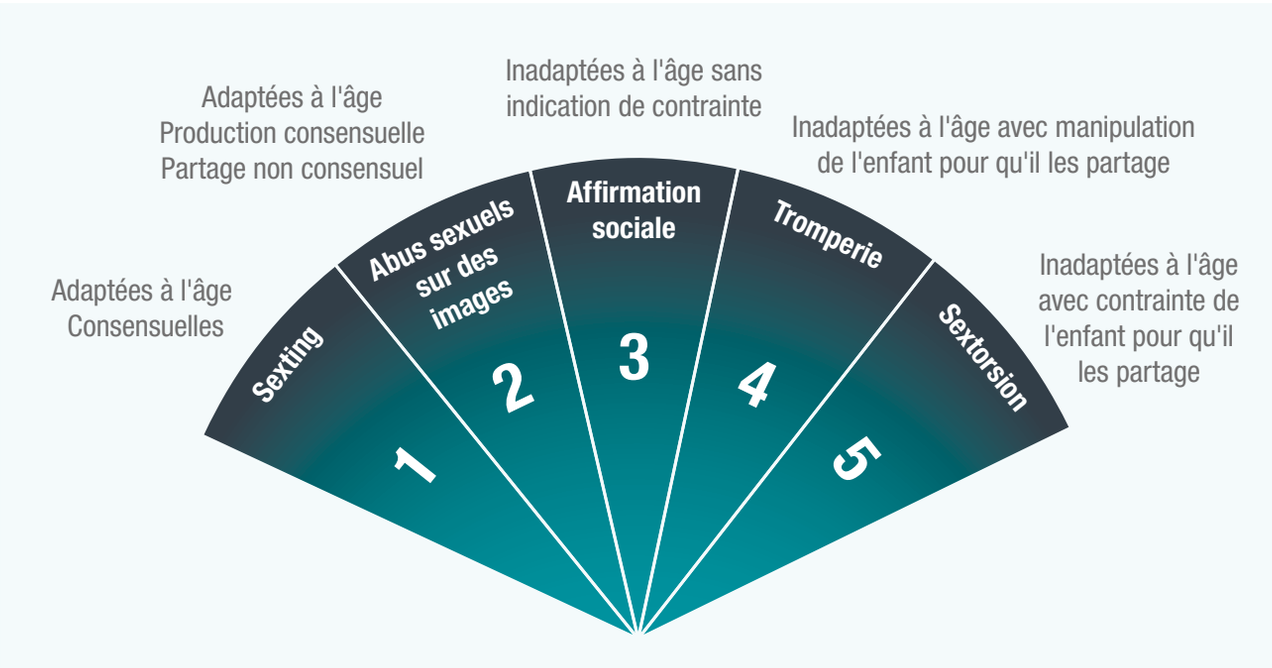
Pour attirer des enfants, ils créaient des faux profils sur des réseaux sociaux et des sites vidéos populaires parmi les enfants, puis ils utilisaient des vidéos pré-enregistrées de victimes mineures antérieures, se livrant souvent à des activités explicitement sexuelles, pour convaincre des enfants qu'ils étaient en train de discuter en direct avec un autre mineur.

Ces vidéos contraignaient et incitaient les enfants à se livrer à des activités explicitement sexuelles devant leur propre webcam, qui pouvaient ensuite être visionnées en direct par de multiples membres adultes à l'insu de la victime. Des membres des sites Internet classaient leurs efforts respectifs pour attirer des enfants sur le site Internet et les contraindre à se livrer à des activités explicitement sexuelles. Un total estimé de 1 500 mineurs ont été attirés sur les sites Internet.[104]

Les risques associés aux abus entre pairs et à l'exploitation perpétrée par des moins de 18 ans, et les risques associés à ce groupe lorsque ses membres deviennent adultes, ont également été identifiés comme une menace émergente.

Il existe des différences distinctes par rapport à l'âge relatif des participants, le degré de consentement/contrainte, et l'intention criminelle des personnes partageant et recevant les images. Cependant, dans tous les cas, il existe un risque élevé que des images indécentes auto-générées et des vidéos d'enfants soient obtenues et partagées en ligne.

Illustration 9 : Catégorisation des images indécentes auto-générées



1. **Les sextos** font référence à la production et au partage **adaptés à l'âge et consensuels** d'images à caractère sexuel entre deux adolescents ou jeunes gens, avec un niveau supposé de confiance que ces images resteront privées entre les parties. Il existe un risque que ces images soient partagées par d'autres sans consentement.
2. **« Les abus basés sur des images »** (également connus sous l'appellation « d'images indécentes non consensuelles » font référence à la production et au partage **adaptés à l'âge** d'images à caractère sexuel entre deux adolescents ou jeunes gens, quand les images sont **partagés publiquement sans consentement**.
3. **« L'affirmation sociale »** fait référence à la **diffusion en direct de performances sexuelles et à caractère sexuel d'enfants** devant une webcam dans le but de collecter des « likes » et de la reconnaissance. En règle générale, les sujets sont très impliqués et ne semblent pas percevoir que leur conduite constitue un rapport sexuel préjudiciable.
4. **« La tromperie »** fait référence à la situation où un enfant est **dupé par un adulte ou adolescent** pour lui faire croire qu'il est impliqué dans une production et un partage consensuels d'images à caractère sexuel avec des pairs d'un âge adapté. Le conspirateur séduit les enfants afin qu'ils adoptent une conduite explicitement sexuelle devant leur propre webcam, qui peut ensuite être visionnée en direct, à l'insu de la victime, par des individus ayant un intérêt sexuel pour les enfants. Cette conduite évolue souvent vers (5).
5. **« La sextorsion »** fait référence au processus par lequel des adultes ou adolescents **séduisent, contraignent ou manipulent** un enfant afin qu'il se livre à une activité sexuelle devant sa webcam afin d'obtenir du matériel plus explicite à partager avec d'autres délinquants. Il existe un risque plus élevé de déviance dans la mesure où le délinquant croit souvent pouvoir faire ça en toute impunité. La profondeur du traumatisme de la victime est intensifiée du fait des sentiments d'auto-accusation et de culpabilité résultant du chantage et de l'extorsion.

Le nombre d'images indécentes auto-générées a augmenté de manière significative au cours des deux dernières années, qu'elles aient été produites de manière consensuelle ou qu'elles résultent d'une manipulation ou d'une contrainte. Au cours des six premiers mois de 2019, l'IWF a répondu à 22 484 signalements de matériel pédopornographique auto-généré en ligne (soit précisément un tiers de tous les signalements ayant entraînés une action pendant cette période.)[105] Un peu plus d'un sixième de ces images ont été classées dans la catégorie de gravité la plus importante (voir ci-dessous).

16 % Des images impliquent une activité sexuelle avec pénétration et/ou des images impliquent une activité avec un animal ou du sadisme

25 % Des images impliquent une activité sexuelle sans pénétration

58 % D'autres images indécentes

Sur l'ensemble des signalements, 96 % concernaient des filles, 2 % concernaient des garçons et 2 % concernaient des filles et des garçons ensemble. Sur l'ensemble des images, plus de 10 % des images représentant des filles et presque 20 % de celles représentant des garçons, concernaient des enfants âgés de 7 à 10 ans.

Âge	Filles (96 %)	Garçons (2 %)
Moins de 7 ans	0,7 %	4,8 %
7-10	10,4 %	19,8 %
11-13	84,5 %	67,7 %
Plus de 13 ans	4,4 %	7,7 %

Le nombre réel de sujets âgés de 13 à 18 ans est peut être plus élevé, dans la mesure où l'IWF ne bloquent pas les images quand ils ne peuvent pas déterminer si le sujet est âgé de moins de 18 ans.

La criminalisation du partage d'images sexuelles par des jeunes gens a des conséquences involontaires, avec le risque que des sociétés qualifient par inadvertance des enfants qui partagent des images « sextos » de manière inappropriée de « dangereux délinquants sexuels » alors que, dans la plupart des cas, leur « crime » est la naïveté. Cependant, les comportements sexuels préjudiciables par des jeunes gens sont un domaine qui requiert beaucoup plus d'attention et des recherches commencent à se focaliser sur ce groupe de population, qui a besoin de soutien et d'interventions thérapeutiques.

La relation changeante des enfants avec la technologie accroît le risque

Deux cas survenus au Pérou montrent la manière dont la technologie peut influencer l'exploitation sexuelle des enfants en ligne.

Dans un cas, un délinquant partageait du matériel pédopornographique avec un autre individu sur des réseaux sociaux. Lors de son arrestation, il a avoué qu'une femme lui avait envoyé le matériel pédopornographique depuis le Pérou. Pendant l'enquête, des magistrats ont trouvé le téléphone portable de la mère de la victime. Il contenait des photographies et des vidéos dans lesquelles elle abusait sexuellement de l'un de ses filles, puis envoyait ces matériels par e-mail et par d'autres réseaux sociaux à un contact à l'extérieur du Pérou.

Dans un autre cas, un sujet âge de 16 ans rencontre un homme de 44 ans par le biais d'une application LGBTQ+. Le délinquant a demandé des photos nues du mineur et lui a demandé d'avoir un rapport sexuel. En raison de sa grande vulnérabilité, l'enfant lui a envoyé ses photos et, sous l'influence du délinquant, ils se sont rencontrés et se sont livrés à des activités sexuelles. Ensuite, le délinquant a harcelé la victime pour la rencontrer de nouveau.[106]

Diffusion en direct à la demande

Des éléments de preuve montrent qu'Internet est utilisé non seulement pour faciliter les transactions et la traite sexuelle, mais également pour la traite d'enfants spécifiquement destinée à satisfaire la demande de sexe virtuel. Ceci est rendu possible par le fait que certaines cultures considèrent que le sexe virtuel cause un préjudice moindre parce que l'abus est perpétré à distance. Une étude récente portant sur 300 enfants philippins qui avaient été victimes d'abus sexuels en ligne a établi que l'exploitation derrière une webcam était considérée comme une « avancée » par rapport à l'exploitation sexuelle dans la rue.[107] Des parents impliqués dans l'exploitation sexuelle d'enfants en ligne (dont certains sont conditionnés par des agresseurs qui leur font découvrir le sexe virtuel) estimaient que cela ne causait pas de préjudice à leurs enfants dans la mesure où il n'y avait aucun contact physique direct entre l'agresseur et la victime.

Les tendances à la traite à des fins de sexe virtuel ont entraîné des appels pour distinguer la traite sexuelle d'enfants de la traite en général dans la loi, avec la mise en œuvre de sanctions plus sévères en raison de la nature double du crime.

07 Le contexte socio-environnemental

Des différences criantes entre le Nord et le Sud créent une discordance mondiale inquiétante

Des facteurs liés à l'environnement local peuvent accroître la vulnérabilité et rendre difficile l'établissement d'une définition commune au niveau international de ce qui constitue un abus, ainsi qu'augmenter la difficulté pour trouver une quelconque réponse internationale pour protéger les enfants, l'identification et l'arrestation des délinquants.

La forte augmentation de l'accessibilité à Internet a accru le risque d'exploitation sexuelle des enfants en ligne dans de nombreux pays où la technologie des portables et du haut débit sont encore des innovations récentes, et où les ressources de soutien, l'éducation, les directives et les mesures de protection nécessaires pour la combattre ne sont pas encore arrivées à maturité technique. Par conséquent, il y aura un nombre croissant de jeunes gens dans les nations en voie de développement qui utiliseront Internet sans avoir conscience des risques qu'ils encourent en ligne ou des services de soutien disponibles au niveau international.

Facteurs environnementaux et éducation

Bien que les facteurs socio-économiques et les inégalités de richesse lient les victimes et leurs vulnérabilités comme cela a été discuté dans le chapitre 6, dans le Nord, il y a eu des investissements beaucoup plus importants pour éduquer les enfants à la sécurité en ligne et aux relations sexuelles. Par ailleurs, des organisations de la société civile sont régulièrement consultées pour établir des politiques gouvernementales et elles offrent des lignes d'assistance confidentielles aux enfants vulnérables. Cependant, le développement technologique continue à prendre de vitesse la capacité des gouvernements à soutenir, éduquer et réglementer la sphère technologique.

Ce problème est plus prononcé mais non exclusif au Sud, où un grand nombre d'usagers obtiennent la propriété d'un dispositif et l'accès à Internet dans un contexte ou des facteurs comme la pauvreté et l'inégalité augmentent l'exposition des enfants à l'exploitation sexuelle. Par exemple, la promesse d'une stabilité financière peut inciter des familles à faible revenu à exposer leurs propres enfants à l'exploitation et aux abus sexuels. L'effondrement du soutien familial peut aboutir à ce que des enfants finissent dans la rue, où l'absence de mesures de protection et de réseaux de soutien peuvent accroître leur vulnérabilité à la traite et à l'exploitation sexuelle dans le cadre de voyages et du tourisme. Bien que les moteurs de l'exploitation sexuelle des enfants en ligne dans les pays en voie de développement n'aient pas fait l'objet de recherches suffisantes, l'UNICEF suggère que la vulnérabilité des enfants en ligne reflète fidèlement celle hors ligne.[108]

Démasquer les agresseurs

En 2015, un délinquant kényan a été condamné à la perpétuité pour avoir participé au site Internet d'exploitation sexuelle des enfants en ligne Dreamboard. Le délinquant a avoué avoir posté 121 messages sur le site - un tableau d'affichage en ligne privé et réservé aux membres qui promouvait l'exploitation sexuelle des enfants en ligne et encourageait l'abus et l'exploitation sexuels d'enfants très jeunes dans un environnement conçu pour éviter d'être repéré par les services de répression. Le délinquant était considéré comme un membre « super VIP » de Dreamboard, une appellation donnée aux membres qui occupaient une position proéminente sur le site et produisait leur propre matériel pédopornographique.

Les poursuites résultaient de l'opération DELEGO, une enquête lancée en décembre 2009 qui visait des individus dans le monde entier pour leur participation à Dreamboard. Elle a abouti à l'inculpation d'un total de 72 individus répartis sur cinq continents. À ce jour, 49 délinquants ont soit plaidé coupable soit été condamnés suite à un procès. Les condamnations s'échelonnent entre cinq ans d'emprisonnement et la perpétuité.[109]

Définir l'exploitation sexuelle des enfants en ligne, la réglementer et légiférer à son sujet

Bien que l'éducation et les ressources de soutien soient utiles pour accroître le niveau de connaissance numérique parmi les enfants et les familles à un niveau national, les efforts internationaux pour lutter contre l'exploitation sexuelle des enfants en ligne sont entravés par une terminologie de base inadéquate et une réglementation et une législation qui ne les soutiennent pas efficacement.

La Convention des Nations Unies relative aux droits de l'enfant (1989) et le protocole facultatif à la Convention relative aux droits de l'enfant sur la vente d'enfants, la prostitution enfantine et la pédopornographie (OPSC, 2000) sont les instruments juridiques internationaux les plus complets qui promeuvent et protègent les droits de l'enfant et protègent les enfants de la vente, de l'exploitation sexuelle et des abus sexuels. Cependant, ces traités ont été adoptés à une époque où les technologies de la communication et les services Internet étaient beaucoup moins développés et répandus, et où les délits sexuels contre des enfants ne présentaient pas le lien étroit avec l'environnement numérique qui prévaut à l'heure actuelle.

Le 30 mai 2019, le Comité des droits de l'enfant des Nations Unies a adopté ses toutes premières directives portant sur le protocole facultatif sur la vente des enfants, la prostitution enfantine et la pédopornographie (OPSC), afin qu'il soit plus facile pour les États-nations de comprendre ce qui est attendu d'eux en termes de mise en œuvre et de conformité.[110]

Le seul traité régional qui traite en détail de la manière dont les États-nations doivent empêcher les délits sexuels à l'encontre des enfants, poursuivre les agresseurs et protéger les enfants victimes est la Convention relative à la protection des enfants contre l'exploitation sexuelle et les abus sexuels du Conseil de l'Europe, connue sous le nom de Convention Lanzarote.[111] Ses normes ont inspiré des changements dans la législation et les politiques de pays dans le monde entier. Elles incluent la directive de l'Union européenne relative à la lutte contre les abus sexuels et l'exploitation sexuelle, qui fournit un cadre législatif holistique couvrant la définition des délits, de l'enquête et des poursuites, de la prévention et de l'aide aux victimes.[112] La Convention Lanzarote a également inspiré la Cour interaméricaine des droits de l'homme, qui a établi une jurisprudence importante en matière de protection de l'enfant, et le Comité africain d'experts sur les droits et le bien-être de l'enfant, qui a élaboré une expérience et une expertise pour s'attaquer aux problèmes importants tels que la vente des enfants et le mariage des enfants.[113]

Néanmoins, des définitions incohérentes au niveau mondial rendent difficile tout accord international quant à ce qui constitue une exploitation sexuelle des enfants en ligne. Subséquemment, des divergences réglementaires et législatives ont créé des vides juridiques qui permettent aux délinquants d'échapper aux services de répression et d'exploiter des enfants vulnérables.

Les défis présentés par l'apport de preuve d'exploitation pour retirer les images

Le Bureau du commissaire australien à la sécurité sur Internet a souligné qu'une recherche sur Internet du nom légal d'un délinquant, ainsi que le surnom de sa fille dans du matériel pédopornographique, révélait des images qui sont toutes des recadrages de son visage issus de matériel représentant des abus sexuels où elle apparaît. Cependant, il est difficile d'obtenir leur retrait quand ces images recadrées ne montrent pas d'abus sexuels.

La tendance récente des enfants à mettre en ligne des films les représentant dansant sur YouTube est devenue populaire auprès des délinquants qui ont laissé des commentaires faisant référence aux parties des vidéos qu'ils trouvaient les plus excitantes. L'algorithme du service a commencé à produire des sélections de ce contenu et à les promouvoir auprès des délinquants.

La ligne de signalement nationale canadienne pour signaler une exploitation sexuelle d'enfants en ligne a découvert qu'ils devaient prouver qu'une image représentait un enfant plutôt que le contraire. S'il existe le moindre doute qu'une image puisse représenter un adulte (ce qui est commun pour les plus de 13 ans), obtenir son retrait est particulièrement difficile.[114]

Disparité des législations internationales

Les définitions des délits varient considérablement d'un pays à l'autre. Les délits associés aux matériels pédopornographiques sont généralement, mais pas exclusivement, clairement définis dans des pays présentant de hauts niveaux d'utilisation d'Internet et inclus des considérations associées aux crimes rendus possibles par Internet. Cependant, dans les pays où l'adoption d'Internet est récente, il y a souvent une absence de définitions légales. Par exemple, à la date de 2018, les matériels pédopornographiques ne sont pas définis dans la législation de Bosnie-Herzégovine, de Chine, d'Indonésie, du Liban, du Pérou, d'Arabie Saoudite, de Singapour ou du Vietnam, pour ne citer que quelques exemples.[115]

De récentes recherches menées par l'ICMEC comparant les normes législatives dans le monde entier avec leur législation nationale modèle ont établi que bien que 118 pays possèdent une législation suffisante pour lutter contre les matériels pédopornographiques, la force de cette législation varie grandement d'un pays à un autre.[116]

L'ICMEC analyse la progression de la législation relative aux matériels pédopornographiques dans chaque pays du globe tous les deux ans et offre des concepts qui devraient être pris en considération lors de l'élaboration d'une législation anti-matériels pédopornographiques.

Les critères principaux du rapport consistent à évaluer si la législation nationale :

1. existe eu égard spécifiquement aux matériels pédopornographiques ;
2. fournit une définition des matériels pédopornographiques ;
3. criminalise les délits associés aux matériels pédopornographiques facilités par la technologie ;
4. criminalise le fait de posséder sciemment des matériels pédopornographiques, avec ou sans l'intention de les distribuer ;
5. requiert des fournisseurs d'accès à Internet qu'ils signalent les matériels pédopornographiques suspectés au services de répression ou à une autre agence mandatée.

Le rapport de 2018[117] montre que :

Nombre de pays	Critères
118	pays possèdent une législation suffisante pour lutter contre les délits associés à des matériels pédopornographiques (satisfont au moins quatre des cinq critères)
21	pays satisfont l'ensemble des cinq critères
16	pays ne possèdent aucune législation traitant spécifiquement des matériels pédopornographiques
51	pays ne définissent pas les matériels pédopornographiques
25	pays ne possèdent pas de dispositions pour les délits associés aux matériels pédopornographiques facilités par la technologie
38	pays ne criminalise pas le fait de posséder sciemment des matériels pédopornographiques, avec ou sans intention de les distribuer

Cette disparité est renforcée par une tendance observée de condamnations moins sévères pour les délinquants en ligne dans les pays du côté de la demande (qui dirige ou cause les abus ou l'exploitation sexuelle en direct en chargeant et payant des délinquants en personne à violer des enfants) par rapport aux délinquants qui commettent des abus par contact « en personne ».

Un rapport du programme philippin de la mission de justice internationale souligne que cette tendance semble :

- amoindrir la gravité de leurs délits liés à l'exploitation et aux abus sexuels graves, répétés et parfois violents des enfants

- échouer à rendre justice aux victimes vulnérables, y compris celles de nations en voie de développement pauvres
- échouer à suffisamment refréner ces délinquants
- être moins susceptible de dissuader la population de délinquants.[118]

Les délinquants en ligne sont les cerveaux et portefeuilles derrière les abus perpétrés par des contacts en personne et doivent être punis, refrénés et dissuadés en conséquence. Dans les faits, ils incitent les abus par contact et les commettent par procuration, et sont donc responsables du fait qu'ils se soient produits. Les délinquants « du côté de la demande » dirigent et causent des abus ou de l'exploitation sexuels en direct en chargeant et payant des délinquants en personne pour violer des enfants d'âges spécifiques, à des moments spécifiques, de manières spécifiques. Ils produisent des matériels pédopornographiques chaque fois qu'ils dirigent et regardent des abus en direct à distance, et ils incitent, sollicitent et contraignent des mineurs à produire des vidéos et des images au contenu sexuel explicite à des fins de consommation ou de distribution.

Toutefois, les pays ayant de faibles niveaux d'utilisation d'Internet ne sont pas les seuls à peiner à définir les matériels pédopornographiques de manière adéquate. Même dans les pays armés de lois solides, des magistrats rencontrent des difficultés pour déterminer des sanctions appropriées et cohérentes pour des combinaisons de délits (comme la séduction, la diffusion en direct, le partage de matériels pédopornographiques et le chantage). De plus, le fait qu'Internet estompe la distinction entre violence physique et en ligne peut permettre à des délinquants d'échapper à la loi. Par exemple, avant que des poursuites ne puissent être lancées, dans la plupart des pays, les lois relatives à la séduction en ligne existantes requièrent que la communication soit suivie d'une rencontre ou d'une intention claire de rencontrer un enfant, malgré le nombre croissant de cas de séduction en ligne où le délinquant semble n'avoir aucune intention de rencontrer l'enfant en personne.[119] Au lieu de ça, son objectif est de recevoir ou d'envoyer des images indécentes auto-générées. Bien que la production, la possession et la distribution de tels matériels soient toutes illégales, des vides juridiques permettent que des captures d'écran de tels contenus soient partagées même après l'identification et le retrait d'Internet de l'original.[120]

Le ciblage des délinquants par le biais de services de répression multinationaux

En 2018, dans le cadre d'une enquête multinationale menée par Interpol, la sécurité intérieure américaine et des autorités thaïlandaises et australiennes, neuf délinquants ont été arrêtés pour avoir utilisés et facilités l'exploitation d'un site du Dark Web qui hébergeait des matériels pédopornographiques.

Le site comptait 63 000 usagers dans le monde entier et présentait des abus de plus de 100 enfants, le plus jeune à avoir été identifié n'étant âgé que de 15 mois. En dépit de leurs efforts draconiens pour rester anonymes, les enquêteurs ont quand même été en mesure de remonter jusqu'aux délinquants et de les identifier.

Le principal administrateur du site abusait son neveu afin de réaliser des contributions au site et a par la suite été condamné à 146 années d'emprisonnement. Un autre délinquant, qui était également un administrateur du site et un enseignant en école maternelle, a été condamné à 40 ans, un record en Australie pour un délit associé à des matériels pédopornographiques. Au moins 50 enfants ont été identifiés et sauvés d'abus depuis le lancement de l'opération, et des efforts pour identifier et secourir d'autres enfants sont en cours.[121,122]

Une proposition de définition de base

Interpol joue le rôle de leader dans les efforts internationaux pour établir une définition « de base » universelle de l'exploitation sexuelle des enfants en ligne, basée sur des critères qui seraient estimés irréfutables par toutes les nations.[123] Les critères proposés :

- la victime est un enfant réel ;
- la victime est pré-pubaire, ou présente les tous premiers signes de la puberté (en règle général, de moins de 13 ans) ;
- les images véhiculent soit :
  - une activité sexuelle de l'enfant, avec l'enfant, en présence de l'enfant, entre enfants ; ou
  - un gros plan sur le vagin, le pénis ou la région anale de l'enfant ; et
- l'image est vérifiée par plusieurs experts de différents pays.

Réglementation des préjudices en ligne

Parmi les nations du Nord, des gouvernements, des organisations des services de répression, l'industrie de la technologie et le secteur tertiaire coopèrent de plus en plus pour trouver des solutions innovantes afin de limiter la diffusion de violences en ligne.

Des progrès ont été accomplis dans certains pays, y compris en Australie, en Allemagne et au Royaume-Uni, pour améliorer la sécurité en ligne en introduisant une réglementation plus stricte d'Internet. Créé en 2015, le Commissaire australien à la sécurité en ligne (eSafety Commissioner) est l'organisme de réglementation, l'éducateur et le coordonnateur en matière de sécurité en ligne, couvrant un large éventail de préjudices. En avril 2018, les États-Unis d'Amérique ont adopté un loi connue sous le nom de « FOSTA » qui a modifié la loi relative à la décence des communications pour exempter les fournisseurs de services de la section 230 sur l'immunité de toute responsabilité pour la publication d'informations fournies par des tiers pour des services qui facilitent sciemment ou soutiennent la traite sexuelle.[124] Par ailleurs, l'Union européenne a annoncé qu'elle allait réviser le changement d'une immunité équivalente fournie par la directive relative au commerce en ligne.[125] Cependant, Internet n'est pas entravé par les frontières nationales et les systèmes légaux. Le défi repose dans la conception d'un nouveau cadre réglementaire pour gérer un problème mondial qui n'a pas de normes ou de définitions acceptées au niveau international.

En avril 2019, le gouvernement britannique a publié un livre blanc sur les violences en ligne, qui a proposé d'établir un organisme national pour réglementer les contenus préjudiciables et faire du Royaume-Uni l'endroit le plus sûr au monde pour aller en ligne.[126] En juillet, suite à un sommet de deux jours sur les menaces actuelles et émergentes pour la sécurité nationale et mondiale, des ministres d'État britanniques, australiens, canadiens, néo-zélandais et américains ont réaffirmé leur engagement à travailler avec l'industrie pour s'attaquer à un éventail de menaces pour la sécurité, y compris l'exploitation sexuelle des enfants en ligne. De plus, pendant une table ronde avec des sociétés du secteur technologique, des ministres ont insisté sur le fait que les efforts des agences de répression pour enquêter sur les crimes les plus graves et les poursuivre seraient entravés si l'industrie met à exécution ses projets d'implémentation de chiffrement de bout en bout sans les garde-fous nécessaires.[127]

La dichotomie de l'état de droit

Alors que les pays où l'état de droit est plus faible créent davantage d'opportunités pour les délinquants d'exploiter des enfants vulnérables, les pays possédant un état de droit fort et des infrastructures sophistiquées sont responsables de l'hébergement d'une proportion substantielle des matériels pédopornographiques en ligne, y compris les Pays-Bas et les États-Unis d'Amérique, qui sont les deux pays où le plus de matériels pédopornographiques sont hébergés à destination de publics mondiaux. L'adoption rigoureuse de mesures de protection des données personnelles dans les nations où l'état de droit est fort a permis l'hébergement en ligne sûr de matériels pédopornographiques.

Il est déjà apparent que la demande de retrait des barrières qui empêchent les services de répression d'avoir accès à des communications privées va entrer en collision avec des inquiétudes mondiales sur la confidentialité en ligne. L'IWF a souligné que demander aux fournisseurs de services Internet de surveiller activement leurs réseaux afin de repérer des contenus illicites entrerait directement en conflit avec l'article 15 de la Directive de l'Union européenne relative au commerce en ligne.[128] À l'heure actuelle, les sociétés privées n'ont aucune obligation de partager des données relatives à des abus sur leurs plateformes ou qui leur ont été signalés, ou concernant les mesures qu'elles ont prises pour protéger les enfants impliqués.

La frustration grandissante du public à l'égard du rôle des fournisseurs de services Internet en tant que catalyseurs d'un vaste éventail de préjudices en ligne va sans doute attirer une attention croissante sur les réglementations relatives aux données personnelles dans la décennie à venir. Les décisions en matière de politiques accroissant le chiffrement et l'anonymat auront un impact crucial sur l'exploitation sexuelle d'enfants en ligne et sur notre capacité à lutter contre elle.

La coopération internationale est impérative pour lutter contre la gravité, l'ampleur et la complexité croissante des délits

En 2019, 337 personnes ont été arrêtées dans 38 pays, y compris au Royaume-Uni, aux États-Unis, en Irlande, en Corée du Sud, en Allemagne, en Espagne, en Arabe Saoudite, aux Émirats arabes unis, en république tchèque et au Canada par rapport à un site d'abus d'enfants sur le Dark Web appelé « Welcome To Video ».

Le site, exploité par un délinquant de 23 ans originaire de Corée du Sud, contenait plus de 250 000 vidéos d'abus, et ses utilisateurs avaient procédé à plus d'un million de téléchargements de matériels pédopornographiques. Le site Internet commercialisait l'abus sexuel d'enfants et était l'un des premiers à offrir des vidéos d'abus graves à la vente en utilisant la crypto-monnaie Bitcoin. Le site a été fermé par un groupe de travail international mis sur pied par la NCA et qui incluait des enquêtes du département de la Sécurité intérieure et du Service des revenus intérieurs des États-Unis, la police nationale de Corée du Sud et la police criminelle fédérale allemande.

Nikki Holland, directrice des enquêtes pour la NCA, a déclaré : « Les délinquants pédophiles du Dark Web - dont certains figurent parmi les pires délinquants - ne peuvent pas échapper à l'attention des services de répression. Ils ne sont pas aussi masqués qu'ils le pensent ; ils ne sont pas aussi en sécurité qu'ils le pensent. »

Ce cas illustre ce que les services de répression constatent en matière de délits associés aux abus sexuels des enfants : une gravité, une ampleur et une complexité accrue, y compris un lien direct entre le visionnage d'images d'abus et les abus par contact, ainsi que des délinquants qui se servent du Dark Web et du chiffrement pour dissimuler leurs activités et leur identité.[129]

08 La sphère du préjudice

Le traumatisme associé aux abus en ligne a un impact énorme et de plus en plus souvent à vie sur les victimes, leur famille et la société

Les quatre focales comprenant les tendances mondiales de la technologie, la menace posée par les délinquants, la vulnérabilité des victimes et le contexte socio-environnemental convergent toutes pour donner naissance à une cinquième focale : le préjudice.

Le traumatisme associé aux abus en ligne a un impact énorme et de plus en plus souvent à vie sur les victimes et leur famille, ainsi que sur les coûts sociaux énormes pour la fourniture de traitements médicaux, d'aide sociale et de soutien à la santé mentale. L'exploitation sexuelle des enfants en ligne a été associée à des défis en matière de santé mentale à un stade ultérieur de la vie, à la dépression, à un risque accru de toxicomanie et à de graves troubles du comportement. Ceci a un impact non seulement sur la victime, mais également sur son réseau familial proche et sur les systèmes de santé et de soutien sociaux/nationaux.

Une étude de 2017 menée par l'Institut national de la justice américain a établi que des enfants ayant des antécédents d'abus physiques et émotionnels étaient plus susceptibles de présenter des troubles du comportement au milieu de leur enfance, ce qui pourrait par la suite aboutir à un comportement criminel à l'âge adulte. Les effets semblent se présenter de manières différentes chez les filles et chez les garçons, les premières ayant tendance à intérioriser les problèmes qui se manifestent alors sous la forme d'anxiété, de dépression et d'isolement social, tandis que les garçons et les jeunes hommes tendent à extérioriser les problèmes, avec une hostilité, une agressivité et une délinquance accrues. Il a été montré que les deux types de comportement aboutissent à un comportement criminel à l'âge adulte et sont liés à des problèmes dans les domaines des études, de l'emploi, de la productivité et des perspectives financières.[130]

Il existe des défis spécifiques dans les pays où, pour des raisons légales et socio-culturelles, les victimes masculines d'abus sexuels sur enfant sont marginalisées aux yeux de la société et/ou de la loi, ou ne sont pas crues ou soutenues même quand elles révèlent les abus.

Calcul du coût de l'exploitation sexuelle des enfants en ligne

Selon le réseau de prévention des crimes sexuels finlandais, le coût d'un crime sexuel se monte à 15 000 € pour les soins médicaux et de thérapie par victime.[131] Europol a indiqué qu'il s'agit d'une estimation très prudente, dans la mesure où elle n'inclut pas le coût à vie des préjudices subis. Cependant, sur les trois mêmes années, une thérapie préventive pour le délinquant ne coûte que 9 600 €.

Coût d'un crime sexuel envers un enfant sur trois ans	
Coûts de l'enquête préliminaire	3 000 €
Coûts du système judiciaire	5 000 €
Peine d'emprisonnement de 2 à 5 ans	121 600 €
Coûts du programme « STOP » en prison	4 300 €
Coûts médicaux pour une victime	5 500 €
Coûts de la thérapie pour une victime sur trois ans	9 600 €
TOTAL	**149 000 €**
Coûts de la thérapie préventive sur trois ans	9 600 €

Une étude universitaire a placé le coût économique de l'abus sexuel des enfants aux États-Unis à l'échelle de la vie à environ 9,3 milliards de dollars américains, y compris les coûts associés aux dépenses gouvernementales et aux pertes de productivité.[132]

Jürgen Stock, le secrétaire général d'Interpol, a déclaré : *« L'ampleur de ce crime est choquante et est aggravée par le fait que ces images peuvent être partagées en ligne à l'échelle mondiale d'une simple pression de touche de clavier et peuvent exister pour toujours. Chaque fois qu'une image ou un clip vidéo est partagé ou visionné, l'enfant est revictimisé. »*[133]

L'histoire d'Olivia, telle qu'elle a été relatée dans le rapport annuel de l'Internet Watch Foundation (Fondation pour la surveillance d'Internet au R-U) de 2018, décrit tous les détails de l'impact et du traumatisme de la revictimisation dans la mesure où les images de son abus sont malheureusement restées en circulation.

L'histoire d'Olivia : l'impact continu de l'abus

Âgée de trois ans, Olivia aurait dû s'amuser avec des jouets et profiter d'une enfance innocente. Au leu de ça, elle a subi des abus sexuels épouvantables pendant plusieurs années et a été violée et torturée sexuellement de manière répétée.

Au bout de cinq ans, la police a porté secours à Olivia. Bien que les abus physiques aient pris fin et que l'homme qui lui avait volé son enfance ait été emprisonné, les images étaient toujours en circulation et des délinquants continuent à partager et sans doute à tirer profit du calvaire d'Olivia. Depuis qu'elle a été secourue, l'image d'Olivia est apparue en ligne cinq fois chaque jour ouvré.

Pour avoir discuté avec ceux qui avaient souffert de revictimisation, nous savons qu'il s'agit d'une torture mentale qui peut briser des vies et rendre difficile le dépassement des abus.

Savoir qu'une image de votre souffrance est partagée et vendue en ligne est déjà assez difficile comme ça. Mais pour les survivants, craindre de pouvoir être identifiés ou reconnus à l'âge adulte est terrifiant.[134]

Un autre défi croissant est la peur de la victime de révéler ce qui lui arrive ou, dans certains cas, en raison de leur jeune âge, un manque de compréhension de ce qui est mal, éventuellement parce les abus ont été perpétrés par un agresseur au sein de la cellule familiale ou qui occupe une position de confiance. Il peut exister un certain nombre de facteurs contributifs, y compris la peur de ne pas être cru, la peur de la permanence (c'est-à-dire que les images et les messages associés resteront toujours en ligne), et des sentiments de honte, d'embarras et de culpabilité. Marie Collins, la fondatrice de la Fondation Marie Collins et une victime d'abus sexuels dans son enfance, a longuement évoqué ces sentiments : *« Enfant, je n'aurais jamais parlé à qui que ce soit des abus que je subissais parce que si j'avais parlé à quelqu'un, il aurait pu les trouver. Je ne voulais vraiment pas que quelqu'un les trouve parce qu'il aurait alors constaté la personne horrible que j'étais... mais je m'inquiétais en permanence de ces images... où elles étaient et qui les avaient vues. »*[135]

Cette peur de la permanence est bien réelle et la revictimisation est une considération relativement récente qui est amplifiée par les abus en ligne. Des images continuent à circuler pendant des années après la période originelle des abus, même après que la victime a été secourue et le délinquant attrapé et poursuivi.

Reconnaissant que nous commençons à présent à voir la première génération des victimes d'images d'abus sexuels d'enfants dont les abus ont fait l'objet d'une distribution en ligne atteindre l'âge adulte, l'enquête sur les survivants internationaux du Centre canadien pour la protection de l'enfant cherche à mieux comprendre les impacts de ce crime et à déterminer quels changements politiques, législatifs et thérapeutiques sont nécessaires pour répondre au besoins de ces victimes.[136]

Le Phoenix 11

Le Phoenix 11 est un groupe de onze survivants dont les abus sexuels subis quand ils étaient enfants ont été enregistrés et, dans la majorité des cas, distribués en ligne. Les membres du Phoenix 11 se sont regroupés afin de former une force puissante pour remettre en cause les réponses inadéquates à la prévalence des images d'abus sexuels d'enfants sur Internet.

En février 2018, le Centre canadien pour la protection de l'enfant, ainsi que le Centre national américain pour les enfants disparus et exploités (NCMEC), ont organisé la première retraite pour ce groupe unique de survivants en Amérique du Nord. Son objectif est de fournir aux survivants un endroit où ils puissent partager certains des défis auxquels ils sont confrontés ou ont été confrontés, et un environnement favorable, afin qu'ils puissent réseauter et nouer des relations avec d'autres survivants. Un résultat a été l'établissement d'un groupe de défense du groupe, le Phoenix 11, qui entend s'efforcer faire entendre la voix collective des victimes et des survivants sur la scène internationale afin d'opérer des changements.

Le centre canadien apporte son aide et son soutien aux efforts du Phoenix 11 pour militer en faveur de changement en rédigeant des lettres en leur nom, en facilitant l'utilisation de leur Déclaration d'impact communautaire lors de procédures judiciaires et en sollicitant leurs commentaires sur les matériels éducatifs et autres destinés à des publics externes.[137]

La technologie constitue également une opportunité de mettre fin aux abus

Dans un monde où un nombre croissant d'enfants possèdent des comptes sur les réseau sociaux et passent une portion de plus en plus importante de leur temps en ligne, la question de savoir comment les protéger au mieux revêt une importance cruciale. Bien qu'il incombe aux gouvernements d'établir des lois et de mettre en œuvre des politiques dans leurs juridictions, ils ne peuvent pas mener ce combat seuls. Les entreprises du secteur privé, les communautés locales, les organisations qui développent la technologie pour repérer et retirer les contenus et les médias ont tous un rôle déterminant à jouer.

Le rapport du groupe de travail technique de l'Alliance pour la dignité de l'enfant inclut la recommandation que l'industrie doit être fortement encouragée à, voire avoir l'obligation, par le biais de la législation domestique, de/d' :

- avoir l'obligation de scruter leurs réseaux, plateformes et services, ou de prendre des mesures actives similaires, comme procédure opérationnelle par défaut, pour repérer les matériels pédopornographiques connus, y compris les services dits « intermédiaires »
- imposer des normes et codes de conduites pour lutter contre les comportements illégaux sur leurs plateformes
- mettre en œuvre des structures où la sécurité est intégrée, des codes de pratique ou des normes minimales.[138]

Revictimisation

En août 2019, un journaliste masculin et une collègue ont contacté la fondation Aarambh, qui héberge le portail de signalement en Inde, pour leur communiquer les URL de contenus vidéo où ils apparaissaient alors qu'ils étaient encore enfants. La détresse éprouvée par les victimes en voyant émerger des contenus en ligne sur leur enfance, ainsi que la stigmatisation sociale associée, avaient un effet direct sur leurs vies, y compris leurs travails, leurs mariages et leurs relations sociales. En examinant des rapports produits par les services de répression locaux en Inde, les organisations ont été en mesure de vérifier le signalement et leur âge, et d'assurer le retrait des URL délictueuses.[139]

En raison de l'émergence de nouveaux défis à mesure que des entreprises privées et des plateformes de réseaux sociaux évoluent vers des communications plus sécurisées et un chiffrement de bout en bout, une action à l'échelle mondiale sera nécessaire pour garantir que des nouvelles technologies puissent être utilisées pour identifier et gérer des contenus illégaux et préjudiciables.

L'intelligence artificielle et l'apprentissage automatique par les machines jouent un rôle crucial dans le « gros œuvre » de la détection d'images et vidéos préjudiciables à une grande échelle. Ceci réduit le préjudice de la revictimisation et permet à des experts formés de concentrer leurs efforts plus efficacement et donner la priorité à l'examen des domaines appropriés. Pour autant, ils n'apportent pas une réponse complète. Par exemple, la génération actuelle des modèles d'apprentissage automatique rencontre des difficultés pour reconnaître le visage, l'âge et le sexe des enfants de différentes origines raciales, ce qui constitue certaines des lacunes sur lesquelles la communauté technologique mondiale devrait se concentrer.

Projet Arachnid

Géré par le Centre canadien pour la protection de l'enfant, le projet Arachnid est un outil innovant pour lutter contre la prolifération croissante de matériels pédopornographiques et repérer où ces images/vidéos sont rendues disponibles au public.

La plateforme du projet Arachnid a initialement été conçue pour parcourir des liens et des sites signalés au préalable à Cybertip.ca pour contenir des matériels pédopornographiques et repérer où ces images/vidéos sont rendues disponibles au public. Une fois que des matériels pédopornographiques ont été repérés, une notification était envoyée au fournisseur hébergeant le contenu pour exiger son retrait.

Le projet Arachnid continue à se livrer aux activités de balayage décrites ci-dessous, mais il évolue et s'adapte en permanence pour améliorer ses capacités à accélérer la détection de matériels pédopornographiques, facilitant ainsi leur retrait rapide.

Au cours de ses trois premières années d'exploitation, le projet Arachnid a traité les volumes suivants :

- 2 milliards de pages Internet scannées contenant plus de 91 milliards d'images. Parmi celles-ci, 13,3 millions étaient suspectes (ce qui signifie matériels pédopornographiques potentiels sur la base d'une analyse réalisée avec PhotoDNA)
- 4,6 millions de notifications de fermeture ont été envoyées à des fournisseurs
- 85 % d'entre elles concernent des victimes qui n'ont pas officiellement été identifiées par la police.[140]

09 Considérations prospectives

Sur la base de notre évaluation de la menace, voici quelques-unes des mesures recommandées que les nations peuvent adopter individuellement ou collectivement pour atténuer l'impact. De plus amples détails sont disponibles dans la Réponse stratégique mondiale à l'exploitation et aux abus sexuels des enfants en ligne, qui est disponible sur le site Internet de l'Alliance mondiale WePROTECT, à l'adresse : https://www.weprotect.org/

Le rapport de l'année en cours montre que l'accès mondial à Internet et aux dispositifs intelligents à bas coût en expansion rapide signifie qu'un nombre plus importants de victimes et de délinquants potentiels arrivent en ligne. Un accès précoce des consommateurs à de nouveaux services de communication sécurisés, avec chiffrement de bout en bout, signifie que les délinquants sont de mieux en mieux protégés dans leur « refuge numérique », avec des niveaux sans précédents de co-opération et de partage d'informations. Les délinquants disposent de multiples canaux pour accéder à une seule occurrence d'abus, et les encouragements de leurs pairs légitiment et normalisent les comportements des délinquants.

Alors même que ces aspects technologiques et sociaux aboutissent à une prolifération des délits et rapprochent les délinquants de leurs victimes, d'autres facteurs sociaux, culturels et économiques qui amplifient le risque et le préjudice sont en jeu. L'âge auquel les enfants sont autorisés à accéder à des réseaux sociaux et à des jeux multi-joueurs en ligne a connu un déclin continu et l'émergence d'un changement des comportements conduit à la normalisation du partage d'images et des comportements sexuels en ligne.

D'importants facteurs contributifs pour gérer ces problèmes à leur échelle actuelle sont la capacité du cadre légale de chaque nation à fournir une protection adéquate aux enfants ; la disponibilité d'un personnel de répression ayant reçu une formation appropriée et qui peut être déployé rapidement et efficacement pour poursuivre les délinquants, et pour localiser et protéger les victimes ; ainsi que leur capacité à impliquer et réglementer l'industrie des technologies afin qu'elle applique les mesures de protection appropriées en vertu de politiques actualisées. Cependant, nous ne devons pas oublier que la responsabilité de l'exploitation sexuelle des enfants en ligne incombe avant tout aux délinquants.

Aujourd'hui, par le biais de l'Alliance mondiale WePROTECT, les États-nations, les organisations de répression, l'industrie de la technologie, les établissements universitaires et le secteur tertiaire peuvent tous devenir des parties intégrantes de la solution mondiale à ce crime odieux contre les personnes les plus vulnérables dans nos sociétés.

Pour lutter contre cette menace persistante et croissante, les nations peuvent prendre certaines mesures individuellement, tandis que d'autres actions doivent être mises en place ensemble :

- ✓ **La communauté internationale** doit davantage prêter attention aux programmes conçus pour empêcher les délits initiaux et la récidive, eu égard aux coûts élevés du soutien thérapeutique aux victimes pendant toute leur vie, et du repérage, des poursuites à l'encontre, de l'incarcération et de la réinsertion des délinquants.
- ✓ **La communauté internationale** doit nouer un dialogue en amont avec les fournisseurs de technologie et de services de manière plus cohérente aux niveaux national et international.
- ✓ **La communauté internationale** doit envisager un changement de paradigme du modèle actuel de signalement et de retrait pour soulager les victimes de leur traumatisme et bannir d'Internet les hébergeurs de mauvais contenus, tout en améliorant l'accès international et le partage de données.
- ✓ **La communauté internationale** doit continuer à élaborer un modèle de classification pour l'exploitation sexuelle des enfants en ligne, en analysant les vides juridiques actuels afin de façonner de nouvelles politiques.
- ✓ L**es sociétés technologiques mondiales** doivent se montrer plus proactives dans leurs efforts pour scruter, repérer et retirer les matériels pédopornographiques, et déjouer les tentatives de séduction, en adoptant une approche fondée sur l'intégration de la sécurité dès la conception plutôt que sur une position réactive par rapport à l'exploitation sexuelle des enfants en ligne, par exemple, par le biais de vérifications du statut des enfants en ligne.
- ✓ **Les nations** possédant une expertise de certains aspects de la réponse nationale modèle doivent avoir le devoir de la partager avec d'autres pays (voir https://www.weprotect.org/the-model-national-response pour obtenir de plus amples informations).
- ✓ **Les nations** doivent se fixer pour objectif de nommer un leader, un éducateur et un régulateur national pour coordonner les efforts de sécurité en ligne et faciliter le retrait des contenus préjudiciables.
- ✓ **Les nations** doivent s'assurer que les réseaux de soutient pour le soutien aux victimes pendant toute leur vie disposent des ressources et des financements adéquats.
- ✓ **Les décideurs nationaux** doivent chercher à adopter une approche équilibrée à l'égard de la législation portant sur la sécurité, la protection de la vie privée et la sécurité publique, en s'assurant que la protection de la vie privée ne réduise ou n'annule pas la capacité des sociétés à rechercher de manière proactive les matériels pédopornographiques ou les comportements de séduction.
- ✓ **Les décideurs nationaux** doivent adopter une approche centrée sur les victimes pour concevoir des campagnes de prévention et des mesures d'intervention, en travaillant avec des agences médiatiques professionnelles et en intégrant les perspectives des victimes ainsi que la voix de jeunes.
- ✓ **Les agences de répression** doivent travailler ensemble pour accroître le partage des technologies sophistiquées et des techniques d'enquête innovantes, afin d'améliorer l'identification des victimes et de contrarier l'exploitation sexuelle des enfants en ligne sur une grande échelle.
- ✓ **Les experts de la sécurité en ligne** doivent partager leurs cadres de meilleures pratiques éducatives, leurs contenus et méthodes d'enseignement, et évaluer leur efficacité en matière de changement des comportements.
- ✓ **Les prestataires d'aide sociale** doivent se forger une meilleure compréhension des personnes les plus vulnérables ou susceptibles d'être exploitées en ligne, et élaborer des interventions sur mesure pour les soutenir.

10 Notes de fin de document

1 'Online Harms White Paper' (gouvernement britannique, 3) disponible à l'adresse : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591512/HO_DfE_consultation_response_on_CSE_definition_FINAL_13_Feb_2017__2_.pdf (consulté le 1er octobre 2019)

2 WeProtect Global Alliance – Évaluation mondiale de la menace 2018

3 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 1er octobre 2019)

4 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 1er octobre 2019)

5 Projet Arachnid' (Centre canadien pour la protection de l'enfance, données au 1er novembre 2019) disponible à l'adresse : https://projectarachnid.ca/en/#shield)

6 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 1er octobre 2019)

7 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2019: pg. 30)

8 Chiffre cité dans 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018: pg. 3) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019)

9 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2019: pg. 30)

10 Correspondance entre Interpol et le Groupe PA Consulting (2019)

11 National Strategic Assessment (National Crime Agency, 2019: pg. 13)

12 'Association of Sexting with Sexual Behaviours and Mental Health Among Adolescents' dans Jama Paediatrics (Mori et al, 2019) cité dans https://www.huffpost.com/entry/talking-to-your-kid-about-sexting_l_5d408dc8e4b007f9accf9939 (consulté le 1er octobre 2019)

13 Alliance mondiale WeProtect – Évaluation mondiale de la menace 2018

14 Connaissances basées sur des études de cas directes soumises aux chercheurs du groupe PA Consulting par le fonds EVAC, le 15 octobre 2019

15 Connaissances basées sur des études de cas directes soumises aux chercheurs du groupe PA Consulting par le Commissaire australien à la Sécurité en ligne, le 17 octobre 2019

16 'Online Harms White Paper' (gouvernement britannique, 8) disponible à l'adresse : https://wearesocial.com/global-digital-report-2019 (consulté le 1er octobre 2019)

17 Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online', (Broadband Commission: 2019)

18 'Online Harms White Paper' (gouvernement britannique, 8) disponible à l'adresse : https://wearesocial.com/global-digital-report-2019 (consulté le 1er octobre 2019)

19 « La situation des enfants dans le monde 2017 : les enfants dans un monde numérique » (UNICEF, 2017: p. 1)

20 'INHOPE Statistics Report' (INHOPE, 2018: pg. 2)

21 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 11 octobre 2019)

22 'Annual Report 2018' (Internet Watch Foundation, 2019)

23 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile device, social media and E-Commerce' (We Are Social, 2019: pg. 8-63)

24 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile device, social media and E-Commerce'

25 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile device, social media and E-Commerce' (We Are Social, 2019: pg. 8)

26 Estimation attribuée au Dr. Michael Seto, psychologue clinique et judiciaire auprès du groupe Royal Ottawa Healthcare, 'How many men are paedophiles?' cité dans https://www.bbc.co.uk/news/magazine-28526106 (consulté le 1er octobre 2019)

27 'How common is males' self-reported sexual interest in prepubescent children?' (Dombert et al., 2016) et 'The Revised Screening Scale for Pedophilic Interests (SSPI-2): Development and Criterion-Related Validation' (Seto et al. 2015)

28 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 11 octobre 2019)

29 'Annual Report 2018' (Internet Watch Foundation, 2019)

30 Correspondance entre Interpol et le Groupe PA Consulting (2019)

31 WeProtect Global Alliance – Évaluation mondiale de la menace 2018

32 National Strategic Assessment (National Crime Agency, 2019: pg. 13)

33 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

34 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

35 'Teenage Brides Trafficked to China Reveal Ordeal' (New York Times, 2019) disponible à l'adresse : https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (consulté le 1er octobre 2019)

36 Cited in 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

37 'Online Harms White Paper' (gouvernement britannique, 88) disponible à l'adresse : https://wearesocial.com/global-digital-report-2019 (consulté le 1er octobre 2019)

38 'Breaking the Dark Net' (VG, 2017) disponible à l'adresse https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en (consulté le 1er octobre 2019)

39 'The Top 7 Messenger Apps in the World' (Inc., 2018) disponible à l'adresse : https://www.inc.com/larry-kim/the-top-7-messenger-apps-in-world.html

40 'DNS over HTTPS: Why we're saying DoH could be catastrophic' (Internet Watch Foundation, 17 juillet 2019) disponible à l'adresse https://www.iwf.org.uk/news/dns-over-https-why-we%E2%80%99re-saying-doh-could-be-catastrophic

41 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

42 'Draft Council Conclusions on combating the sexual abuse of children' (Conseil de l'Union européenne, 2019) disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-12326-2019-INIT/en/pdf (consulté le 10 octobre 2019)

43 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 29 octobre 2019)

44 'How paedophiles use cookies and keywords to hide sexual abuse images in innocent looking sites' (Independent, 2017) disponible à l'adresse : https://www.independent.co.uk/life-style/gadgets-and-tech/features/paedophilia-child-sexual-abuse-images-video-codes-keywords-clues-cookies-iwf-masking-breadcrumbing-a7661051.html (consulté le 1er octobre 2019)

45 Correspondance entre Interpol et le Groupe PA Consulting (2019)

46 'Teenage Brides Trafficked to China Reveal Ordeal' (New York Times, 2019) disponible à l'adresse : https://www.irishtimes.com/news/crime-and-law/virtual-child-abuse-imagery-a-headache-for-garda%C3%AD-1.3803910 (consulté le 1er octobre 2019)

47 'Online Harms White Paper' (gouvernement britannique, 2018) disponible à l'adresse : https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content (consulté le 1er octobre 2019)

48 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2019: pg. 30)

49 Correspondance de la Mission pour la justice internationale avec le Groupe PA Consulting (2019)

50 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

51 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

52 Cité dans 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 30)

53 Des informations supplémentaires sont disponibles sur le site de la campagne d'EUROPOL 'Trace an Object», disponible à l'adresse : https://www.EUROPOL.europa.eu/stopchildabuse (consulté le 1er octobre 2019)

54 'Online Harms White Paper' (gouvernement britannique, 2019) disponible à l'adresse : https://www.gov.uk/government/news/security-summit-ends-with-pledges-to-tackle-emerging-threats (consulté le 1er octobre 2019)

55 'Etiology of Adult Sexual Offending', dans Sex Offender Management and Planning Initiative at the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (Faupel, S., and Przybylski, R.) disponible à l'adresse : https://www.smart.gov/SOMAPI/sec1/ch2_etiology.html (consulté le 1er octobre 2019)

56 'Towards a Global Indicator: On unidentified victims in child sexual abuse material' (INTERPOL, ECPAT, 2018) disponible à l'adresse https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

57 Base de données INTERPOL ICSE

58 'Mapping Online Child Safety in Asia and the Pacific,' dans Asia and the Pacific Policy Studies, Vol. 5, Issue 3, (Singh, R. D., 2018: pg. 651-664)

59 '#SoSockingSimple wins ISPA best PR campaign' (Internet Watch Foundation, 12 July 2019) disponible à l'adresse : https://www.iwf.org.uk/news/sosockingsimple-wins-ispa-best-pr-campaign

60 'National Strategic Assessment' (National Crime Agency, 2019: pg. 12)

61 Correspondance entre Interpol et le Groupe PA Consulting (2019)

62 « La situation des enfants dans le monde 2017 : les enfants dans un monde numérique » (UNICEF, 2017: p. 1)

63 Présentation dans le cadre de la conférence du Policing Institute for the Eastern Region (PIER) 'Tackling Online Child Sexual Exploitation' (Anglia Ruskin University, 25-26 avril 2019) by Marcella Leonard (experte en thérapie psychosexuelle, et protection de l'enfant et du public) www.leonardconsultancy.co.uk

64 Correspondance entre Interpol et le Groupe PA Consulting (2019)

65 Correspondance entre Interpol et le Groupe PA Consulting (2019)

66 Correspondance entre le ministère de l'Intérieur britannique et le Groupe PA Consulting (2019)

67 Correspondance de la Mission pour la justice internationale avec le Groupe PA Consulting (2019)

68 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing Exploited Children, 2018) disponible à l'adresse : https://www.icmec.org/child-pornography-model-legislation-report/ (consulté le 1er octobre 2019)

69 Correspondance entre Interpol et le Groupe PA Consulting (2019)

70 'Interpol network identifies 10,000 child sexual abuse victims' (Interpol, 2018) disponible à l'adresse : https://www.csacentre.org.uk/csa-centre-prod/assets/File/CSE%20perpetrators%202%20-%20Characteristics%20and%20motivations%20of%20perpetrators%20of%20CSE.pdf (consulté le 1er octobre 2019)

71 'Interpol network identifies 10,000 child sexual abuse victims' (Interpol, 2017) disponible à l'adresse : https://www.basw.co.uk/system/files/resources/basw_64920-4.pdf (consulté le 1er octobre 2019)

72 “A review of the evidence for female sex abusers” (McCloskey & Raphael, 2005), cité dans ‘Who Abuses Children?’ (Australian Government Institute of Family Studies CFCA Resource Sheet, 2014) disponible à l’adresse : https://aifs.gov.au/cfca/publications/who-abuses-children (consulté le 1er octobre 2019)

73 Données NCMEC, fournies par INTERPOL, 5 septembre 2019

74 ‘Interpol network identifies 10,000 child sexual abuse victims’ (Interpol, 2018) disponible à l'adresse : https://www.iwf.org.uk/news/iwf-global-figures-show-online-child-sexual-abuse-imagery-up-by-a-third (consulté le 19 octobre 2019)

75 ‘Interpol network identifies 10,000 child sexual abuse victims’ (Interpol, 2019) disponible à l'adresse : https://supchina.com/2019/07/24/china-vows-to-take-a-hardline-on-child-sexual-abuse/ (consulté le 1er octobre 2019)

76 ‘Online Harms White Paper’ (gouvernement britannique, 2019) disponible à l'adresse : https://www.chinadailyhk.com/articles/233/225/172/1542599418213.html (consulté le 1er octobre 2019)

77 Correspondance du fonds End Violence Against Children (EVAC) (Mettre fin à la violence contre les enfants) avec les secrétariat du WPGA et le Groupe PA Consulting (2019)

78 Correspondance du fonds End Violence Against Children (EVAC) (Mettre fin à la violence contre les enfants) avec les secrétariat du WPGA et le Groupe PA Consulting (2019)

79 1‘Child sexual abuse images on the internet: a cybertip.ca analysis’ (Canadian Centre for Child Protection, 2016) disponible à l'adresse : https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (consulté le 1er octobre 2019)

80 Correspondance du fonds End Violence Against Children (EVAC) (Mettre fin à la violence contre les enfants) avec les secrétariat du WPGA et le Groupe PA Consulting (2019)

81 « La situation des enfants dans le monde 2017 : les enfants dans un monde numérique » (UNICEF, 2017: p. 1) « La situation des enfants dans le monde 2017 : les enfants dans un monde numérique » (UNICEF, 2017: p. 1)

82 ‘How safe are our children?’ (NSPCC, 2019)

83 Chiffres cités dans ‘Studies in Child Protection: Technology-Facilitated Child Sex Trafficking’ (International Centre for Missing and Exploited Children, 2018: pg. 10) Chiffres cités dans ‘Studies in Child Protection: Technology-Facilitated Child Sex Trafficking’ (International Centre for Missing and Exploited Children, 2018: pg. 10)

84 Chiffres cités dans ‘Studies in Child Protection: Technology-Facilitated Child Sex Trafficking’ (International Centre for Missing and Exploited Children, 2018: pg. 10) Chiffres cités dans ‘Studies in Child Protection: Technology-Facilitated Child Sex Trafficking’ (International Centre for Missing and Exploited Children, 2018: pg. 10)

85 Chiffres cités dans ‘Studies in Child Protection: Technology-Facilitated Child Sex Trafficking’ (International Centre for Missing and Exploited Children, 2018: pg. 10) Chiffres cités dans ‘Studies in Child Protection: Technology-Facilitated Child Sex Trafficking’ (International Centre for Missing and Exploited Children, 2018: pg. 10)

86 ‘Fortnite Frenzy Key Findings’ (Common Sense Media, 2018) disponible à l'adresse : https://www.commonsensemedia.org/fortnite-frenzy-key-findings (consulté le 1er octobre 2019)

87 Correspondance entre le ministère de l'Intérieur britannique et le Groupe PA Consulting (2019)

88 ‘Sexual Exploitation of Children in Cambodia Submission for the Universal Periodical Review of the human rights situation in Cambodia’ (APLE Cambodia, ECPAT International 2018)

89 Chiffre cité dans ‘The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report’ (Terre des Hommes, 2018: pg. 6) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019) ‘Online Harms White Paper’ (gouvernement britannique, 6) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019)

90 Chiffre cité dans ‘The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report’ (Terre des Hommes, 2018: pg. 6) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019) ‘Online Harms White Paper’ (gouvernement britannique, 11) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019)

91 ‘Sexual Exploitation of Children in Cambodia Submission for the Universal Periodical Review of the human rights situation in Cambodia’ (APLE Cambodia, ECPAT International 2018: pg. 4)

92 https://projectarachnid.ca/en/#faq (consulté le 3 novembre 2019)

93 ‘Understanding African Children’s use of ICT; A youth-lead survey to prevent sexual exploitation Online’, (ECPAT International, 2013) cité dans ‘The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report’ (Terre des Hommes, 2018)

94 Cité dans ‘Sexual Exploitation of Children in Mexico Submission for the Universal Periodic Review of the Human Rights Situation in Mexico (ECPAT Mexico, 2018) disponible à l'adresse : https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Mexico.pdf (consulté le 1er octobre 2019)

95 ‘How safe are our children?’ (NSPCC, 2019: pg. 13)

96 ‘We keep it in our hearts: sexual violence against men and boys in the Syria crisis’ (UNHCR, rapport d’octobre 2017)

97 ‘Teenage Brides Trafficked to China Reveal Ordeal’ (New York Times, 2019) disponible à l'adresse : https://www.nytimes.com/2019/08/17/world/asia/china-bride-trafficking.html (consulté le 1er octobre 2019)

98 ‘Sex Slaves: The Prostitution, Cybersex & Forced Marriage of North Korean Women & Girls in China’ (Korea Future Initiative, 2019) disponible à l’adresse : https://www.koreafuture.org/report/sex-slaves (consulté le 1er octobre 2019)

99 ‘Korean Approaches to Online Protection for Children in Digital Era’ (Jalil, J., 2013) cited in ‘Global study on sexual exploitation of children in travel and tourism’ (ECPAT International, 2016: pg. 27) disponible à l'adresse : https://www.protectingchildrenintourism.org/wp-content/uploads/2018/10/Global-Report-Offenders-on-the-Move.pdf (consulté le 1er octobre 2019) ‘Online Harms White Paper’ (gouvernement britannique, 27) disponible à l'adresse : https://www.protectingchildrenintourism.org/wp-content/uploads/2018/10/Global-Report-Offenders-on-the-Move.pdf (consulté le 1er octobre 2019)

100 1‘Child sexual abuse images on the internet: a cybertip.ca analysis’ (Canadian Centre for Child Protection, 2016) disponible à l'adresse : https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (consulté le 1er octobre 2019)

101 Briefing de l'IWF briefing aux chercheurs de PA Consulting, le 27 septembre 2019

102 Recherches menées par Johnstonbaugh, M., Arizona State University, citées dans ‘Sexting is a normal part of modern dating’, (Daily Mail, 2019) disponible à l'adresse : https://www.dailymail.co.uk/sciencetech/article-7363601/Sexting-normal-modern-dating-NOT-associated-sexually-risky-behavior.html (consulté le 1er octobre 2019)

103 Briefing de l'IWF briefing aux chercheurs de PA Consulting, le 27 septembre 2019

104 Briefing d'Interpol au secrétariat de WePROTECT et aux chercheurs de PA Consulting, le 5 septembre 2019

105 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consulté le 15 octobre 2019)

106 Correspondance de l'Internet Watch Foundation avec le Groupe PA Consulting (2019)

107 Correspondance de End Violence Against Children avec le Groupe PA Consulting (2019)

108 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018: pg. 14) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019) 'Online Harms White Paper' (gouvernement britannique, 14) disponible à l'adresse : https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consulté le 1er octobre 2019)

109 « L'état des enfants dans le monde 2017 : les enfants dans un monde numérique » (UNICEF, 2017: p. 1) « L'état des enfants dans le monde 2017 : les enfants dans un monde numérique » (UNICEF, 2017: p. 1)

110 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consulté le 15 octobre 2019)

111 « Rapport explicatif sur les Directives relatives à la mise en œuvre du protocole facultatif à la Convention relative aux droits de l'enfant sur la vente d'enfants, la prostitution enfantine et la pédopornographie » (ECPAT International, 2019)

112 « Convention relative à la protection des enfants contre l'exploitation sexuelle et les abus sexuels (« la convention Lanzarote ») » (Conseil de l'Europe, 2007)

113 « Directive 2011/93/EU relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants et à la pédopornographie » disponible à l'adresse : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093 (consultée le 3 novembre 2019)

114 « Directives terminologiques : Pour la protection des enfants contre l'exploitation sexuelle et les abus sexuels » (Groupe de travail interorganisations du Luxembourg, 2016)

115 Correspondance entre le commissariat australien à la sécurité en ligne et le Groupe PA Consulting (2019)

116 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing Exploited Children, 2018) disponible à l'adresse : https://www.icmec.org/child-pornography-model-legislation-report/ (consulté le 1er octobre 2019)

117 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing Exploited Children, 2018) disponible à l'adresse : https://www.icmec.org/child-pornography-model-legislation-report/ (consulté le 1er octobre 2019)

118 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing Exploited Children, 2018) disponible à l'adresse : https://www.icmec.org/child-pornography-model-legislation-report/ (consulté le 1er octobre 2019)

119 Correspondance de la Mission pour la justice internationale avec le Groupe PA Consulting (2019)

120 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing Exploited Children, 2018) disponible à l'adresse : https://www.icmec.org/child-pornography-model-legislation-report/ (consulté le 1er octobre 2019)

121 L'exploitation sexuelle des enfants en ligne, une menace mondiale 'Trends in Online Child Sexual Exploitation: Examining the distribution of Captures of Live-streamed Child Sexual Abuse (Internet Watch Foundation, 2018)

122 ‘INTERPOL network identifies 9 child sexual abuse victims’ (INTERPOL, 2019) disponible à l'adresse : https://www.INTERPOL.int/en/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation (consulté le 20 octobre 2019)

123 ‘Fifty children saved as international paedophile ring busted’ (BBC, 2019) disponible à l'adresse : https://www.bbc.co.uk/news/world-48379983 (consulté le 20 octobre 2019)

124 Correspondance entre Interpol et le Groupe PA Consulting (2019)

125 Les lois Fight Online Sex Trafficking Act (FOSTA) (loi relative à la lutte contre la traite sexuelle en ligne) et Stop Enabling Sex Traffickers Act (SESTA) (loi pour ne plus faciliter la tâche des trafiquants sexuels en ligne) sont entrées en vigueur aux États-Unis le 11 avril 2018

126 ‘US, Europe threatens tech industry’s cherished legal ‘shield’’ (Politico, 2018) disponible à l'adresse : https://www.politico.eu/article/tech-platforms-copyright-e-commerce-us-europe-threaten-tech-industrys-cherished-legal-shield/ (consulté le 20 octobre 2019)

127 ‘Online Harms White Paper’ (gouvernement britannique, 2019) disponible à l'adresse : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf (consulté le 20 octobre 2019)

128 ‘Five Country Ministerial communiqué: emerging threats, London 2019’ (gouvernement britannique, 2019) disponible à l'adresse : https://www.gov.uk/government/publications/five-country-ministerial-communique/five-country-ministerial-ommunique-emerging-threats-london-2019 (consulté le 20 octobre 2019)

129 ‘Online Harms White Paper Response’ (Internet Watch Foundation, 2019: pg. 9)

130 ‘337 arrested after takedown of horrific dark web child abuse site Welcome To Video’ (NCA, 2019) disponible à l'adresse : https://nationalcrimeagency.gov.uk/news/337-arrested-after-takedown-of-horrific-dark-web-child-abuse-site-welcome-to-video (consulté le 21 octobre 2019)

131 ‘Effects of Child Maltreatment, Cumulative Victimization Experiences, and Proximal Life Stresses on Adult Crime and Antisocial Behaviour’ (Herrenkohl, T. I. et al., 2017)

132 Preventing Sexual Crimes’ cité dans ‘New and Innovative ways to tackle child sexual abuse’ (Save the Children)

133 ‘The economic burden of child sexual abuse in the United States’ (Letourneau, E. J., et al., 2018: pg. 413-22)

134 ‘Interpol network identifies 10,000 child sexual abuse victims’ (Interpol, 2017) disponible à l'adresse : https://www.INTERPOL.int/en/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims (consulté le 20 octobre 2019)

135 ‘Annual Report 2018’ (Internet Watch Foundation, 2019)

136 Cité dans ‘Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people’ (Barnardo’s and Marie Collins Foundation, 2016: pg. 37)

137 International Survivors’ Survey (Centre canadien pour la protection de l'enfance, septembre 2017), disponible à l'adresse : https://www.protectchildren.ca/en/resources-research/survivors-survey-results/

138 ‘Phoenix 11’ (Centre canadien pour la protection de l'enfance) disponible à l'adresse : https://protectchildren.ca/en/programs-and-initiatives/phoenix11/)

139 Correspondance entre la fondation Aarambh et le Groupe PA Consulting (2019)

140 Projet Arachnid’ (Centre canadien pour la protection de l’enfance, données au 1er novembre 2019) disponible à l’adresse : https://projectarachnid.ca/en/#shield)

Pour en savoir plus,

Vous pouvez trouver de plus amples informations sur notre site Internet
www.weprotect.org

ou nous suivre sur Twitter @weprotect