

# ÉVALUATION MONDIALE DE LA MENACE 2021

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



# Sommaire

- 01** Avant-propos
- 02** Résumé
- 03** Introduction
- 04** Évaluation de l'exposition des enfants aux abus sexuels en ligne et facteurs de risque: conclusions sommaires
- 05** Thèmes:
  - COVID-19
  - Technologie
  - Règlementation, coopération volontaire et transparence
- 06** Agressions:
  - Sollicitation d'enfants à des fins d'exploitation et d'abus sexuels en ligne (ou « grooming »).
  - Production de matériels d'abus sexuels d'enfants
  - Recherche et/ou consultation de matériels d'abus sexuels d'enfants
  - Partage et/ou stockage de matériels d'abus sexuels d'enfants
  - Contenu à caractère sexuel « autoproduit » par les enfants
  - Diffusion en direct d'actes d'exploitation et d'abus sexuels envers des enfants
- 07** Recommandations
- 08** Remerciements
- 09** Glossaire
- 10** Annexe A: Enquête de WeProtect Global Alliance/Technology Coalition sur les entreprises technologiques
- 11** Notes de fin de document

# Avant-propos

## Bienvenue dans la troisième « Évaluation mondiale de la menace » de WeProtect Global Alliance: la première que nous publions depuis notre création en tant qu'entité indépendante en avril 2020.

Au cours de cette période, la COVID-19 a eu un impact sans précédent. Le monde en ligne a pris encore plus de place dans la vie des enfants et, pour les protéger contre l'exploitation et les abus sexuels en ligne, nous devons d'abord comprendre le problème auquel nous sommes confrontés. Pour ce faire, nous devons écouter: les gouvernements, le secteur privé, la société civile et, surtout, les victimes et survivants de ces abus.

Pour la première fois, nous avons interrogé des milliers de jeunes adultes à travers le monde sur leur expérience des agressions sexuelles en ligne. Nous partageons les conclusions exclusives du secteur de la technologie sur sa riposte face à ce crime. Enfin, nous avons recueilli les données de sociétés de sécurité en ligne sur les tendances émergentes. Tout cela, associé à une réponse sans précédent de la part de nos membres, fait de cette évaluation la plus complète que nous ayons réalisée jusqu'à présent.

### Nous avons été frappés par trois observations.

- 1 L'ampleur de l'exploitation sexuelle des enfants en ligne est en progression. Cette hausse soutenue excède notre capacité de riposte à l'échelle mondiale. La violence sexuelle envers les enfants demeure un problème chronique de financement insuffisant. C'est pourquoi nous avons travaillé d'arrache-pied pour créer cette Alliance mondiale. Nous - à savoir 98 gouvernements, 53 entreprises, 61 organisations de la société civile et 9 institutions internationales - reconnaissons tous que la violence sexuelle en ligne envers les enfants est inacceptable. Nous convenons tous de la nécessité de collaborer pour y mettre fin. Cependant, nous savons maintenant qu'il faudra un changement radical dans notre réponse mondiale.
- 2 La prévention doit être prioritaire dans notre réponse. Trop souvent, nous attendons que l'abus ait eu lieu avant d'agir. Une réponse judiciaire et une application stricte de la loi sont indispensables. Mais pour mettre en place une stratégie véritablement durable, nous devons prévenir activement les abus. Il ne s'agit pas seulement de promouvoir la sécurité des enfants en ligne. Cela va au-delà des initiatives comme Safety by Design qui rendent plus difficile l'utilisation des services en ligne par les délinquants, et au-delà de la dissuasion des agresseurs potentiels. La prévention, c'est tout cela et bien plus encore.

- 3 Nous devons nous assurer de créer des environnements en ligne sûrs dans lesquels les enfants peuvent s'épanouir. Des initiatives prometteuses sont déjà en cours, mais il faudra davantage de soutien.
- 4 Il y a de l'espoir. Au cours des dix dernières années, l'exploitation et les abus sexuels en ligne envers les enfants ont progressé dans les priorités mondiales. Un nombre grandissant de pays, d'entreprises et d'organisations de la société civile participent à la lutte contre ce type de criminalité. Les technologies de sécurité en ligne sont plus accessibles et plus avancées. Les gouvernements précisent les responsabilités des prestataires de services en ligne dans la prévention et la lutte contre les abus sexuels sur leurs plateformes, et les font respecter. Le rythme du changement est peut-être plus lent que nous le souhaiterions, mais celui-ci se produit. Notre rôle en tant qu'Alliance est d'encourager les initiatives et de favoriser leur développement.

Pour terminer, nous tenons à remercier le comité directeur du projet, Economist Impact, Crisp, PA Consulting ainsi que les contributeurs parmi nos membres et d'autres pour avoir créé ce document. Vos avis, vos défis et votre engagement ont été inestimables. Nous pensons que les futures évaluations mondiales de la menace montreront comment notre collaboration et notre ingéniosité permettront de surmonter le problème et de garantir aux enfants du monde entier les avantages du monde numérique, sans exploitation ni abus sexuels.



**Iain Drennan**  
Directeur général  
WeProtect Global Alliance



**Ernie Allen**  
Président  
WeProtect Global Alliance

# Résumé

## Aujourd'hui, les enfants sont confrontés à une menace soutenue d'exploitation et d'abus sexuels en ligne.

Notre réponse mondiale à ce crime a besoin d'une approche innovante pour éviter qu'un nombre toujours grandissant d'enfants ne soit en danger et ne subisse le traumatisme des agressions.

La meilleure voie pour effectuer ce changement est l'amélioration de la sécurité en ligne des enfants et la réduction des opportunités pour les délinquants.

Conformément aux précédentes évaluations mondiales de la menace, ce rapport confirme que l'exploitation et les abus sexuels en ligne envers les enfants continuent de se multiplier. **De nombreuses tendances émergentes menacent d'accroître encore le nombre et la complexité des cas**, et d'intensifier les difficultés pour ceux qui s'emploient à réduire le risque et les agressions.

Ce rapport met également l'accent sur les possibilités d'améliorer la réponse dans le cadre d'une approche à plusieurs niveaux. Les organismes réglementaires, les organisations de la société civile, le secteur de la technologie et le système judiciaire ont tous un rôle à jouer.

Figure 1: L'ampleur du problème.





Outre la description de la diversification rapide des agressions associées à la menace, nous examinerons les causes profondes de l'exploitation et des abus sexuels en ligne envers les enfants. La technologie fait maintenant partie de tous les aspects de la vie quotidienne. Malgré cela, nous continuons à tort à différencier notre façon de traiter les abus « en ligne » (par rapport aux abus « physiques »), comme en témoignent les peines réduites pour les infractions « en ligne »<sup>5</sup>. Cela montre à quel point notre réponse n'a pas réussi à évoluer au rythme de la menace.

**Depuis l'Évaluation mondiale de la menace 2019, la nature du danger a continué à prendre de l'ampleur et à se diversifier.**

Au cours des deux dernières années, le signalement de cas d'exploitation et d'abus sexuels en ligne envers les enfants a atteint ses niveaux les plus élevés. Les chiffres indiquent une augmentation des variables suivantes:

- L'incidence des sollicitations ou « grooming » en ligne.<sup>6,7</sup>
- Le volume de matériels d'abus sexuels d'enfants disponible en ligne.<sup>8</sup>
- La distribution et le partage de matériels d'abus sexuels d'enfants.<sup>9</sup>
- La diffusion en direct contre paiement.<sup>10</sup>

**L'ampleur et le rythme du changement sont sans précédent**, comme l'indiquent les données du National Center for Missing and Exploited Children (NCMEC - Centre national pour les enfants disparus et exploités) américain et de l'Internet Watch Foundation (IWF - Fondation pour la surveillance d'Internet).

# +100%

**Augmentation des signalements  
d'exploitation sexuelle en ligne par le public  
(NCMEC)<sup>11</sup>**

De 2019 à 2020.

# 77%

**Augmentation du contenu à caractère sexuel  
autoproduit par les enfants,  
(IWF)<sup>12</sup>**

De 2019 à 2020.

La pandémie de COVID-19 est indéniablement un facteur ayant contribué à la hausse de l'exploitation et des abus sexuels en ligne envers les enfants (voir *COVID-19* dans le chapitre « Thème »). L'augmentation du contenu à caractère sexuel « autoproduit » par les enfants est une autre tendance qui remet en question la réponse actuelle.

**Le plus grand nombre de signalements ne signifie pas nécessairement que la criminalité a augmenté de façon proportionnelle: les causes peuvent être une sensibilisation accrue du public et une détection plus proactive par les prestataires de services en ligne. Néanmoins, le niveau des abus peut être plus élevé que ce qui est suggéré par les données disponibles:**

- 1 L'exploitation sexuelle des enfants est un crime peu signalé<sup>13</sup>. Dans une enquête mondiale réalisée par Economist Impact, 54% des participants ont déclaré avoir subi des agressions sexuelles en ligne pendant leur enfance, notamment par l'envoi de contenu sexuellement explicite ou des sollicitations qui les mettaient mal à l'aise.

Il y a relativement moins de données sur l'ampleur du problème dans les pays du Sud (voir Glossaire). Les estimations des niveaux d'agression et d'exploitation sont susceptibles d'être revues à la hausse à mesure que ce manque de données probantes sera comblé.

- 2 Alors que la plupart des entreprises ayant répondu à l'enquête WeProtect Global Alliance/Technology Coalition utilisent des outils pour détecter le matériels d'abus sexuels d'enfants (la correspondance de hachage des images et des vidéos est utilisée respectivement par 87% et 76% d'entre elles), 37% seulement en emploient pour détecter les sollicitations en ligne. Cela suggère qu'une part importante de ces activités peut ne pas être détectée.<sup>14</sup>

Même les délinquants dotés d'une faible capacité technique peuvent échapper à la détection en utilisant des services de messagerie cryptés et des outils d'anonymat facilement accessibles. À l'autre extrémité de l'échelle, comme l'a souligné Crisp, certains agresseurs sur le Dark Web (voir Glossaire) utilisent des techniques avancées pour masquer leurs activités. L'utilisation de « services cachés » pour distribuer du matériels d'abus sexuels d'enfants, par exemple, a augmenté de 155% entre 2019 et 2020<sup>15</sup>. La détection est probablement faible dans l'ensemble, particulièrement dans les pays où les capacités d'enquête numérique sont réduites.

**Les tendances récentes risquent d'alimenter la croissance soutenue des agressions:**

- Les nouveaux moyens de monétiser le matériels d'abus sexuels d'enfants et le développement du contenu « autoproduit » par les enfants, moyennant paiement dans les deux cas, renforcent les intérêts commerciaux des abus.
- L'augmentation des volumes de matériel « autoproduit » crée des problèmes complexes pour les décideurs.
- Les délinquants diversifient leurs méthodes de production, par exemple en contraignant des enfants à se livrer à des actes sexuels filmés (« capping »). L'Australian Centre to Counter Child Exploitation rapporte que le « capping » est à l'origine d'environ 60 à 70% des signalements à son unité d'identification des victimes.<sup>16</sup>

Ce rapport contribue à établir une image plus précise du comportement des délinquants. Le stéréotype dominant, selon lequel il faut « se méfier des étrangers » n'est pas confirmé par les faits. Les abus sexuels sur les enfants sont souvent perpétrés par des membres de la famille<sup>17 18 19 20</sup>, et ces indications sont exacerbées par les restrictions dues à la COVID-19. Et même si certains délinquants sont motivés par une attirance sexuelle à l'égard des enfants, ils ne représentent pas tous les cas. Selon la Fondation Lucy Faithfull, seuls 15 à 20% des délinquants avec lesquels elle travaille actuellement sont des pédophiles « dans la mesure où ils sont principalement attirés par les enfants prépubères »<sup>21</sup>. Nous devons continuer à approfondir notre compréhension des différentes voies menant à la délinquance, afin de contribuer à la dissuasion et la prévention des abus à l'avenir.

**Nous devons continuer à approfondir notre compréhension des différentes voies menant à la délinquance, afin de contribuer à la dissuasion et la prévention des abus à l'avenir.**

Cette évaluation mondiale de la menace met en évidence les priorités et les opportunités de mettre un frein à la hausse de l'exploitation et des abus sexuels en ligne envers les enfants.

La réponse stratégique mondiale (RSM) élaborée par WeProtect Global Alliance offre une stratégie internationale exhaustive pour éliminer ce fléau.<sup>22</sup>

Elle identifie quatre domaines prioritaires dans le cadre de la réponse:

<b>Priorité/opportunité recommandée:</b>	Règlementation d'Internet
<b>Catégorie RSM:</b>	Politique/législation

Certains projets font évoluer leur législation afin d'inclure des lois qui place la responsabilité juridique sur les prestataires de services Internet.

La réglementation d'Internet a le potentiel de rendre les environnements en ligne plus sûrs pour les enfants. Mais il faudra des cadres juridiques évolués et des consultations approfondies à l'appui pour arriver à atteindre les bons résultats.

<b>Priorité/opportunité recommandée:</b>	Développement de la capacité des services de répression
<b>Catégorie RSM:</b>	Justice pénale

Bien que certains pays bénéficient d'une réponse répressive avancée, de nombreux services de police sont confrontés à des problèmes fondamentaux qui les empêchent de faire face à la menace. La plupart sont sous-financés, sous-équipés et submergés par l'ampleur de la délinquance.

Les gouvernements doivent augmenter leurs investissements dans les services de répression. Cela améliorerait les capacités nationales en matière de politique numérique et permettrait une plus grande collaboration pour lutter contre les infractions transfrontalières et techniquement sophistiquées via la création d'unités d'enquête spécialisées multinationales.

<b>Priorité/opportunité recommandée:</b>	Coopération volontaire, transparence et technologies de sécurité en ligne
<b>Catégorie RSM:</b>	Technologie

Il faudra bien plus qu'une réglementation, une coopération volontaire et de la transparence pour parvenir à la réactivité requise pour faire face à cette menace qui évolue rapidement.

Depuis l'évaluation mondiale de la menace 2019, des mesures significatives ont été prises pour faire respecter les principes d'intégration de la sécurité à la conception (« Security by Design ») par les plateformes et stimuler les investissements mondiaux dans les technologies de sécurité en ligne. Avec les cadres appropriés à l'appui et une application plus large, de telles solutions peuvent renforcer significativement la riposte globale à la menace.

<b>Priorité/opportunité recommandée:</b>	Initiatives sociétales (variées)
<b>Catégorie RSM:</b>	Sociétal

Il faut renouveler l'attention portée à un éventail d'initiatives sociétales, notamment:

- Les interventions visant à donner aux jeunes les moyens de développer des comportements sexuels sains.
- Les initiatives s'attaquant aux causes profondes de l'exploitation et des abus sexuels envers les enfants – par exemple, les attitudes envers les femmes. Une récente analyse des éléments de preuve menée par l'UNICEF révèle que « les facteurs prédictifs les plus forts de l'acceptation des attitudes (à l'égard des abus sexuels sur les enfants) sont... les points de vue soutenant le pouvoir des hommes envers les femmes<sup>23</sup>.
- Les interventions sociétales visant à réduire les stigmates qui empêchent à la fois la divulgation des abus et la recherche d'une assistance de la part des personnes qui risquent de commettre de tels actes.

## **L'exploitation et les abus sexuels en ligne envers les enfants sont l'une des questions les plus urgentes et les plus déterminantes de notre génération.**

Ces priorités recommandées ont le potentiel de faire cesser l'exploitation et les abus sexuels envers les enfants ou de les empêcher de se reproduire. Au sens large, la prévention consiste à:

**Réduire le risque de délinquance**, en identifiant les personnes à risque de commettre des abus, en les aidant à traiter leurs comportements problématiques, et en gérant de près le risque lié aux délinquants condamnés.

**Réduire le risque pour les enfants**. Créer des environnements plus sûrs pour les enfants. La charge de réduire le risque d'agression ne doit pas incomber aux enfants.

**Réduire les risques globalement**, en contrant les facteurs structurels des abus. Une prévention efficace englobe les interventions sociétales qui s'attaquent aux causes profondes de l'exploitation et des abus sexuels envers les enfants.

**La prévention représente la meilleure voie pour assurer la durabilité de la réponse future.**

Celle-ci devrait s'appuyer sur le rôle des services en première ligne pour continuer à riposter aux cas d'abus sexuels, à faire obstacle aux délinquants et à soutenir les victimes et les survivants. La solution consiste à équilibrer les investissements dans la prévention dans le cadre d'une réponse globale et intégrée.

**Ensemble, nous avons les connaissances, les moyens et les possibilités d'agir, d'améliorer la riposte mondiale et d'empêcher que davantage d'enfants soient agressés.**

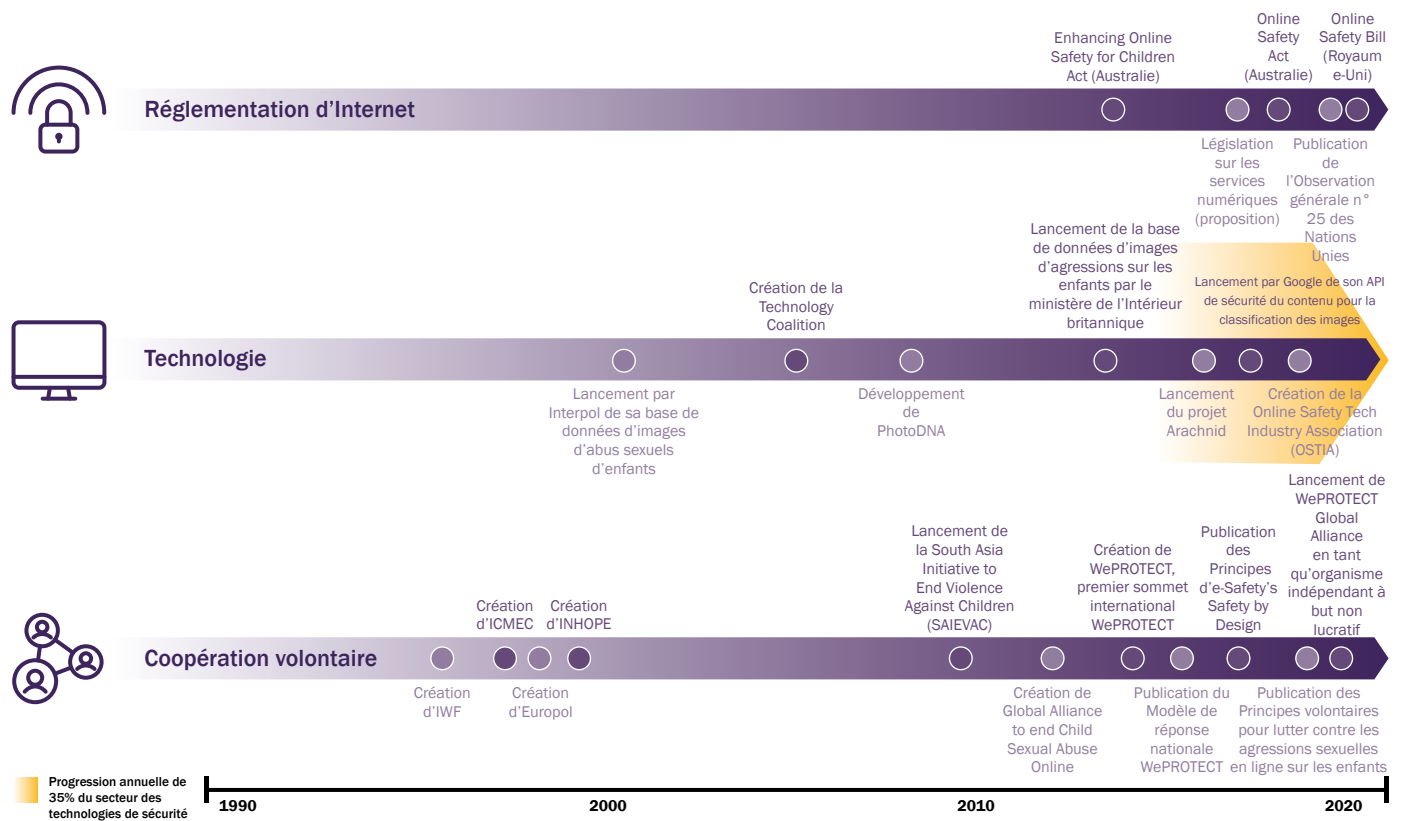
L'exploitation et les abus sexuels en ligne envers les enfants sont l'une des questions les plus urgentes et les plus déterminantes de notre génération. Les nations sont confrontées à des défis différents et en sont à divers stades dans l'évolution de leur réponse à la menace. Certains ont connu une accélération rapide de la connectivité Internet ces dernières années, et la conscience sociétale des méfaits en ligne y est relativement embryonnaire. Dans d'autres, il existe déjà une demande cohérente du grand public en faveur d'une action proactive en vue de résoudre ce problème.

Les solutions technologiques mises en œuvre par les prestataires de services en ligne peuvent créer un avantage mondial, tout comme les approches législatives locales, en incitant les multinationales à améliorer globalement leur transparence, leur responsabilité et leur réactivité. La figure 2 montre les principaux développements réalisés au cours des trois dernières décennies qui ont stimulé la réponse internationale à l'exploitation et aux abus sexuels en ligne envers les enfants. La dynamique sous-jacente à ces évolutions devrait se maintenir à mesure que les services en ligne évoluent et que le grand public partout dans le monde prend conscience de ces agressions et devient moins tolérant.

Les principales recommandations issues de l'évaluation de la menace mondiale 2021 sont détaillées au chapitre 7: *Recommandations*. Bien que les mesures doivent être adaptées et hiérarchisées en fonction du contexte local, il s'agit d'actions que tous les gouvernements et toutes les entreprises et communautés peuvent prendre pour améliorer la riposte à l'exploitation et aux abus sexuels en ligne envers les enfants. Nous avons la responsabilité commune à l'échelle mondiale de travailler ensemble pour protéger les enfants contre de telles agressions. En 2021, nous avons une occasion sans précédent de le faire en maintenant une dynamique mondiale pour transformer notre réponse collective.



Figure 2: Illustration des principaux développements visant à favoriser une réponse préventive accrue.



# Introduction

## DÉFINITIONS

**Abus sexuel sur enfant** désigne « la participation d'un enfant [toute personne âgée de moins de 18 ans] à une activité sexuelle qu'il n'est pas pleinement en mesure de comprendre, à laquelle il ne peut consentir en connaissance de cause ou pour laquelle il n'est pas préparé du point de vue de son développement ». Il s'agit de la définition de la violence sexuelle envers les enfants adoptée par WeProtect Global Alliance (« l'Alliance »), sur la base des lignes directrices de l'Organisation mondiale de la santé (OMS)<sup>24</sup>.

**Exploitation sexuelle des enfants** désigne une forme d'abus sexuel sur un enfant qui implique l'utilisation abusive ou la tentative d'utilisation abusive d'une position de vulnérabilité, de force ou de confiance. Cela comprend, sans s'y limiter, les avantages monétaires, sociaux ou politiques tirés de l'exploitation sexuelle d'une autre personne. Cette infraction peut être perpétrée par des individus ou groupes de délinquants. Ce qui distingue l'exploitation sexuelle des enfants des abus sexuels sur enfants est la notion sous-jacente d'échange présente dans l'exploitation<sup>25</sup>. Les deux concepts se chevauchent fortement, car l'exploitation est souvent une caractéristique de l'abus et vice versa<sup>26</sup>.

**Exploitation et abus sexuels en ligne envers les enfants** désigne l'exploitation et les abus sexuels envers les enfants qui sont partiellement ou entièrement facilités par la technologie, c'est-à-dire par Internet ou d'autres modes de communication sans fil. Ce concept est également désigné par l'abréviation anglaise OCSEA (Online Child Sexual Exploitation and Abuse) et ces agressions sont dites « facilitées par la technologie ».



## Portée

Ce rapport est la troisième évaluation mondiale de la menace publiée par l'Alliance pour décrire l'ampleur et la portée de l'exploitation et des abus sexuels en ligne envers les enfants, et galvaniser la riposte.

D'après les conclusions de l'évaluation mondiale de la menace 2019, les tendances émergentes indiquaient un « raz-de-marée » de l'exploitation sexuelle des enfants en ligne, avec un nombre grandissant de victimes et de survivants dans son sillage<sup>27</sup>. Elle analysait la menace essentiellement à travers quatre prismes: les victimes, les délinquants, les tendances technologiques et le contexte socio-économique.

Le présent rapport adopte une approche fondée sur les agressions pour permettre une exploration plus nuancée des différentes expériences des victimes et des survivants, des méthodes employées par les délinquants, des technologies et des contextes socio-économiques des différentes manifestations de l'exploitation et des abus sexuels en ligne envers les enfants. Ceci est défini à la figure 3: Définition des agressions. Cette approche permet une évaluation plus complète des facteurs en jeu dans chaque agression, ainsi que des possibilités et stratégies d'intervention.

Les agressions étudiées s'entremêlent, comme le montrent la figure 4 et ce rapport.

Nous passons également en revue trois thèmes transversaux:

- COVID-19.
- Technologie.
- Règlementation, coopération volontaire et transparence.

## REMARQUE SUR LA TERMINOLOGIE RELATIVE AUX « AGRESSIONS »

Les « agressions » (définies à la figure 3) décrivent les abus commis par les délinquants. Ces descriptions ne sont pas formulées de façon à refléter les expériences des victimes et survivants. Cette approche a pour but de nous permettre d'explorer les facteurs liés à la délinquance qui sont au cœur de son élimination et de sa prévention. Cette terminologie ne cherche nullement à minimiser l'impact sur les victimes. Celui-ci est aussi analysé parallèlement à chaque agression, y compris dans les études de cas correspondantes.

Figure 3: Définitions des « agressions »

Agression	Définition
<p><b>Sollicitation d'enfants en ligne à des fins d'exploitation et d'abus sexuels</b></p>	<p>Création par un individu d'une relation, d'un sentiment de confiance et d'un lien émotionnel avec un enfant ou un jeune afin de le manipuler, de l'exploiter et d'abuser de lui (ceci étant facilité, partiellement ou entièrement, par Internet ou d'autres modes de communication sans fil)<sup>28</sup>. Il n'y a pas toujours une volonté de rencontre en personne.</p> <p><i>Certaines organisations utilisent le terme d'« incitation en ligne » (tel que défini par le NCMEC<sup>29</sup>) pour faire référence à cette agression.</i></p>
<p><b>Production de matériels d'abus sexuels d'enfants</b></p>	<p>Production de contenu d'abus sexuels d'enfants(voir Glossaire) par des photos/ vidéos/enregistrements audio en personne ; création de contenu textuel ou de matériel visuel non photographique (par exemple, généré par ordinateur) ; ou manipulation de matériels d'abus sexuels d'enfants existant pour créer de nouvelles images inédites.</p>
<p><b>Recherche et/ou consultation de matériels d'abus sexuels d'enfants</b></p>	<p>Recherche, consultation ou tentative de consultation de matériels d'abus sexuels d'enfants sur Internet.</p>
<p><b>Partage et/ou stockage de matériels d'abus sexuels d'enfants</b></p>	<p>Téléchargement, stockage, hébergement et/ou partage de matériels d'abus sexuels d'enfants.</p>
<p><b>Contenu à caractère sexuel « autoproduit » par les enfants</b></p>	<p>Contenu de nature sexuelle, notamment les images et vidéos produites par les enfants eux-mêmes, qui les représentent nus ou partiellement nus. Le contenu à caractère sexuel « autoproduit » par les enfants n'est pas une agression en soi (il peut être produit volontairement et partagé dans le cadre d'un échange approprié sur le plan du développement personnel, par exemple, entre adolescents). Toutefois, il existe des scénarios dans lesquels il y a bien une agression qui est commise, notamment:</p> <ul style="list-style-type: none"> <li>• Lorsqu'un enfant ou un adolescent est contraint de créer du contenu à caractère sexuel « autoproduit ».</li> <li>• Lorsque du contenu à caractère sexuel volontairement « autoproduit » est partagé contre la volonté de l'adolescent.</li> </ul> <p>Le présent rapport examine les caractéristiques de l'« auto-production » préjudiciable. Ce terme figure entre guillemets tout au long du rapport afin d'éviter de présupposer la volonté de l'enfant ou du jeune concerné. Bien que le contenu produit puisse correspondre à la définition du matériels d'abus sexuels d'enfants, l'intention peut être floue et ne peut en aucun cas être considérée comme acquise.</p>
<p><b>Diffusion en direct d'actes d'exploitation et d'abus sexuels envers des enfants</b></p>	<p>Retransmission, en temps réel sur Internet, d'actes d'exploitation ou d'abus sexuels envers des enfants.</p>

## Objectifs

L'objectif principal de ce rapport est de détailler l'ampleur et la portée de la menace de l'exploitation et des abus sexuels en ligne envers les enfants, à l'aide d'une évaluation compréhensible et significative pour tous les publics à travers le monde. Il vise à encourager une action fondée sur des données probantes en reconnaissant les progrès significatifs réalisés à ce jour et en mettant en évidence les possibilités de réduire le risque pour les enfants afin de prévenir les abus.

## Méthodologie

Ce rapport est une méta-étude qui distille les conclusions de plusieurs études internationales afin d'accroître leur portée mondiale, de dresser un tableau global de la menace et d'offrir une évaluation équilibrée dans laquelle les informations ne sont pas complètes et les experts peuvent être en désaccord (avec des réserves, le cas échéant).

Il s'agit d'une étude secondaire étayée par diverses formes d'études primaires:

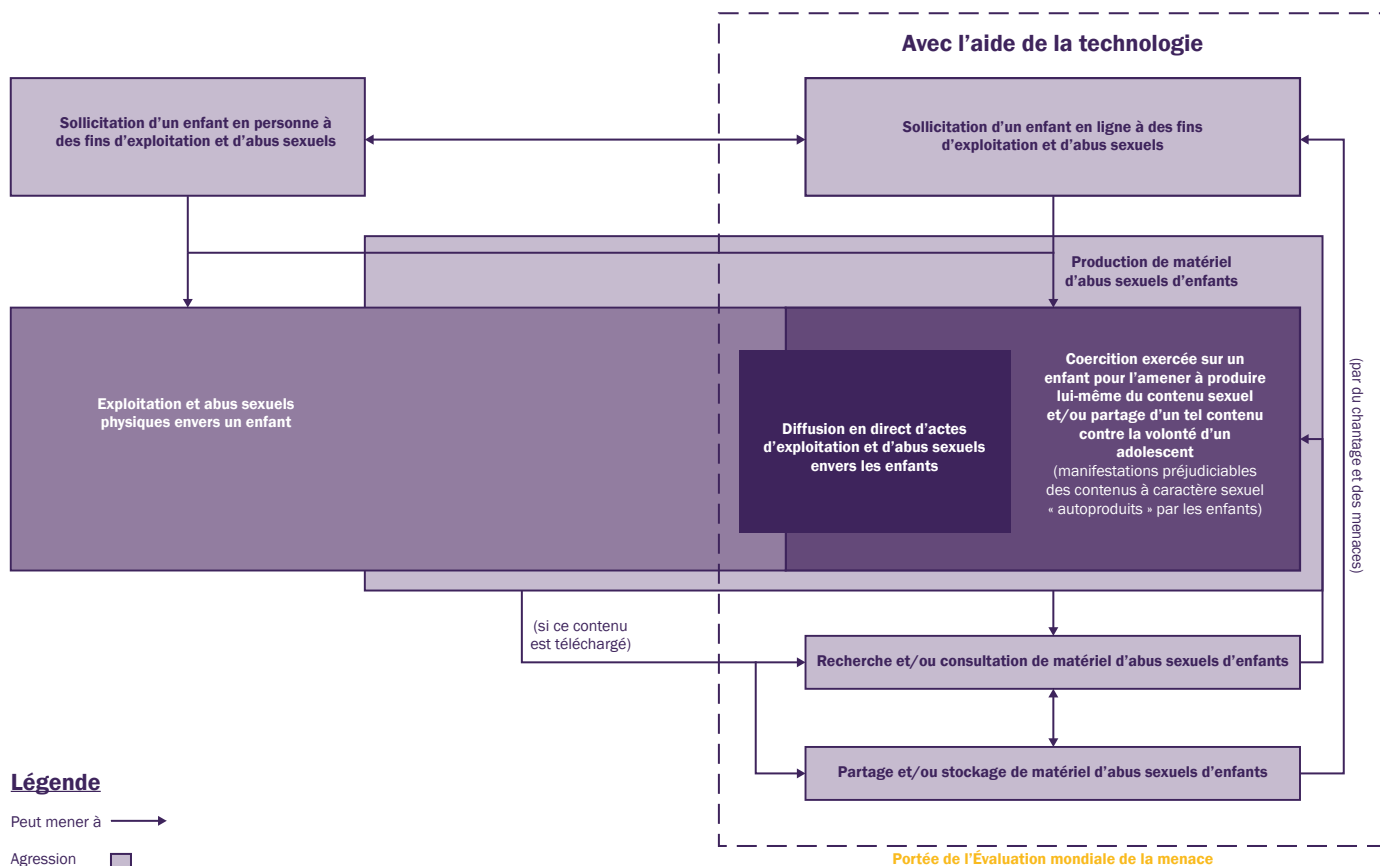
- Entretiens avec des responsables des forces de l'ordre, des défenseurs de la sécurité des enfants, des universitaires, des représentants du secteur de la technologie et d'autres experts.
- Études de cas fournies par les organisations membres et leurs affiliés.
- Une enquête anonymisée auprès de 32 entreprises technologiques mondiales, réalisée par l'Alliance en collaboration avec la Technology Coalition.
- Visuels réalisés par Crisp, l'un des principaux fournisseurs de technologies de sécurité en ligne. Ceux-ci sont inclus dans des encadrés (voir l'exemple à la figure 6).

L'élaboration de ce rapport a été menée par un comité directeur composé de 20 experts issus de services de répression, du gouvernement, du secteur de la technologie, d'organisations non gouvernementales et intergouvernementales (ONG et OIG), et du milieu universitaire (voir page 66).

**CRISP**

Avec sa solution Actor Risk Intelligence, Crisp fournit des renseignements sur les programmes et « techniques de dissimulation » employés par les individus et groupes malveillants, afin de prévenir la délinquance, la désinformation et les abus en ligne. Son outil Actor Intelligence Graph analyse les conversations numériques en temps réel pour révéler les relations entre les acteurs et leurs groupes afin de prévoir les agressions en ligne le plus tôt possible. Crisp protège plus de deux milliards d'utilisateurs quotidiens, dont 450 millions d'enfants environ. [www.crispthinking.com](http://www.crispthinking.com)

Figure 4: Cartographie des agressions.



# Approche de l'étude



**58**

études de cas réalisées



**+230**

articles étudiés



**55**

organisations consultées



**34**

entretiens effectués

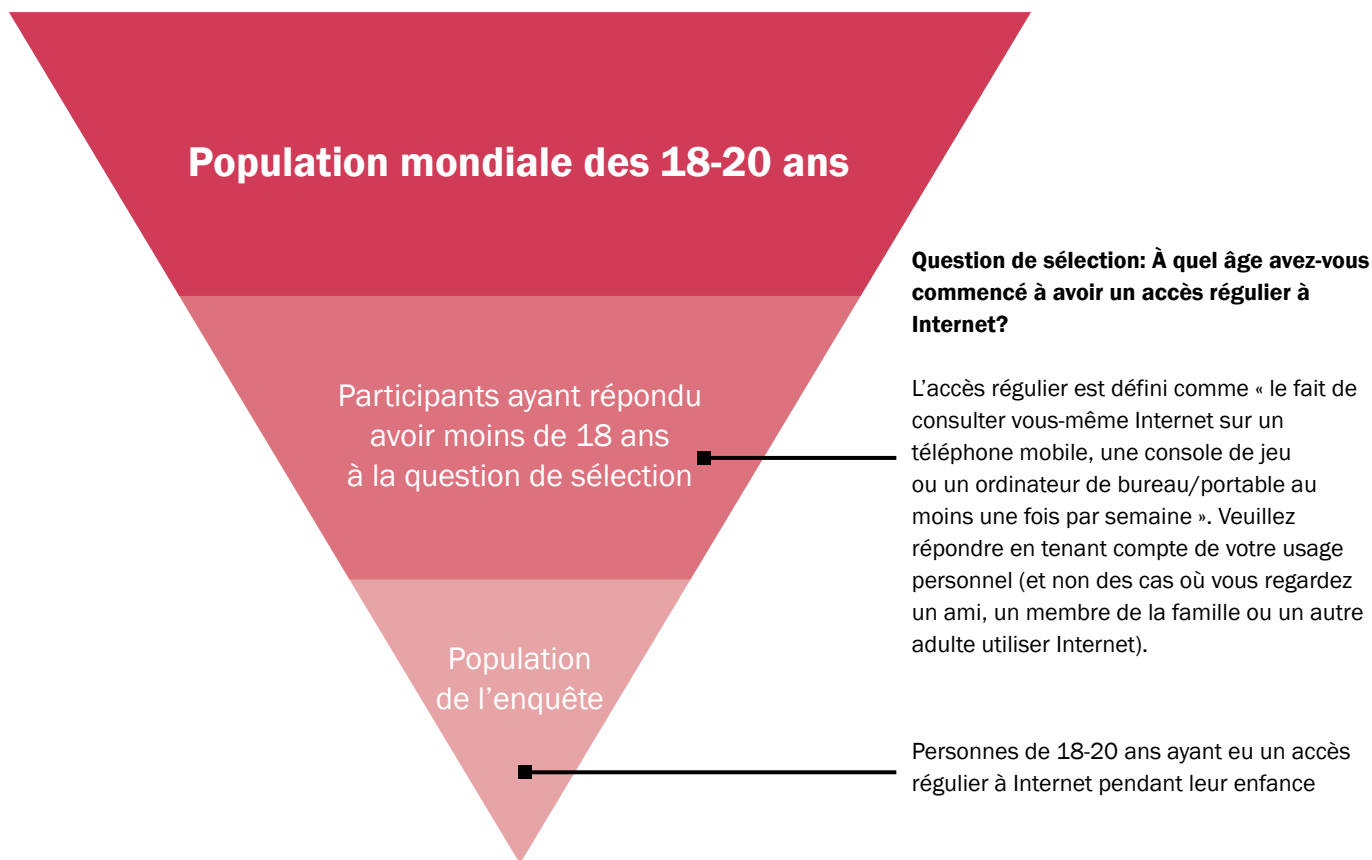
# ECONOMIST IMPACT

## Estimations de l'exposition des enfants aux agressions sexuelles en ligne et facteurs de risque

### UNE ÉTUDE MONDIALE SUR LES EXPÉRIENCES DES JEUNES DE 18 À 20 ANS PENDANT LEUR ENFANCE

**Internet, les réseaux sociaux et autres applications/plateformes numériques peuvent être une épée à double tranchant pour les enfants et les jeunes. Ils constituent des forums de discussion importants pour l'apprentissage et l'interaction, ainsi qu'une plateforme pour explorer positivement la sexualité et favoriser les relations entre enfants<sup>i</sup>. En même temps, ils peuvent être utilisés pour faciliter l'exploitation et les abus sexuels envers les enfants tant par des adultes, de leur connaissance ou non, que par leurs pairs, et permettre aux mineurs d'accéder à un contenu inapproprié pour leur âge.**

Pour combler le déficit mondial de connaissances sur l'ampleur et la portée potentielles des agressions sexuelles envers les enfants en ligne, Economist Impact et WeProtect Global Alliance ont mené une étude qui rassemble des informations fournies par plus de 5 000 jeunes de 18 à 20 ans issus de 54 pays différents, qui avaient régulièrement accès à Internet quand ils étaient enfants<sup>ii</sup>.



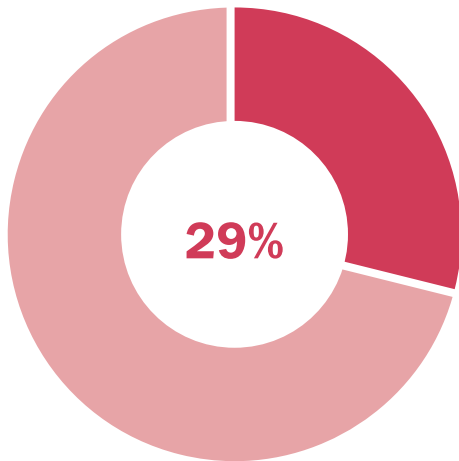
Le questionnaire interrogeait les participants sur leur exposition aux agressions sexuelles en ligne et sur leurs facteurs de risque pendant l'enfance. Les questions portaient essentiellement sur quatre agressions sexuelles en ligne<sup>iii</sup>. Ces agressions sont les suivantes:

- Envoi de contenu sexuellement explicite par un adulte ou quelqu'un qu'ils ne connaissaient pas avant d'avoir 18 ans.
- Demande de garder le secret sur une relation sexuellement explicite en ligne avec un adulte ou quelqu'un qu'ils ne connaissaient pas auparavant.
- Partage d'images sexuellement explicites d'eux-mêmes sans leur consentement (par un de leurs pairs, un adulte ou une personne qu'ils ne connaissaient pas auparavant).
- Demande (par un de leurs pairs, un adulte ou une personne qu'ils ne connaissaient pas auparavant) d'accomplir un acte sexuellement explicite en ligne qui les rendait mal à l'aise.

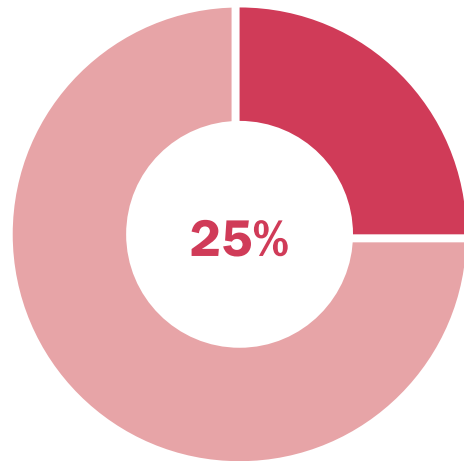
Les principales conclusions de cette étude sont présentées ci-dessous. Les résultats complets et la méthodologie peuvent être consultés dans *Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18 to 20 year olds* sur le site *WeProtect Global Alliance*.

## CONCLUSIONS PRINCIPALES

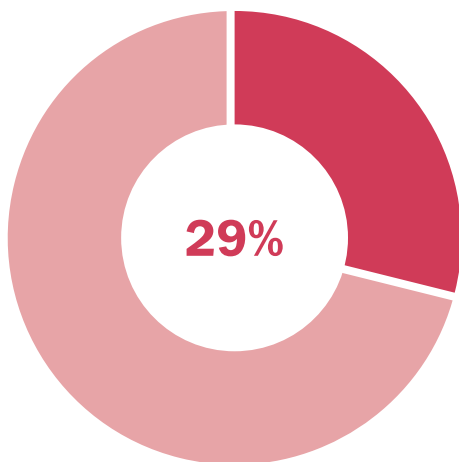
**54%** des participants ont subi au moins une agression sexuelle en ligne au cours de leur enfance<sup>iv</sup>.



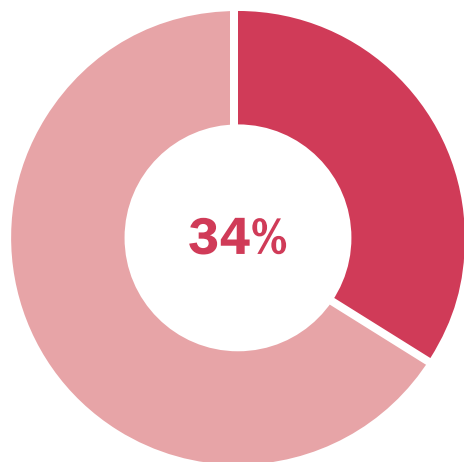
**ont reçu du contenu sexuellement explicite de la part d'un adulte de leur connaissance ou non avant l'âge de 18 ans**



**se sont vu demander, par un adulte de leur connaissance ou non, de garder le secret sur des échanges en ligne sexuellement explicites**



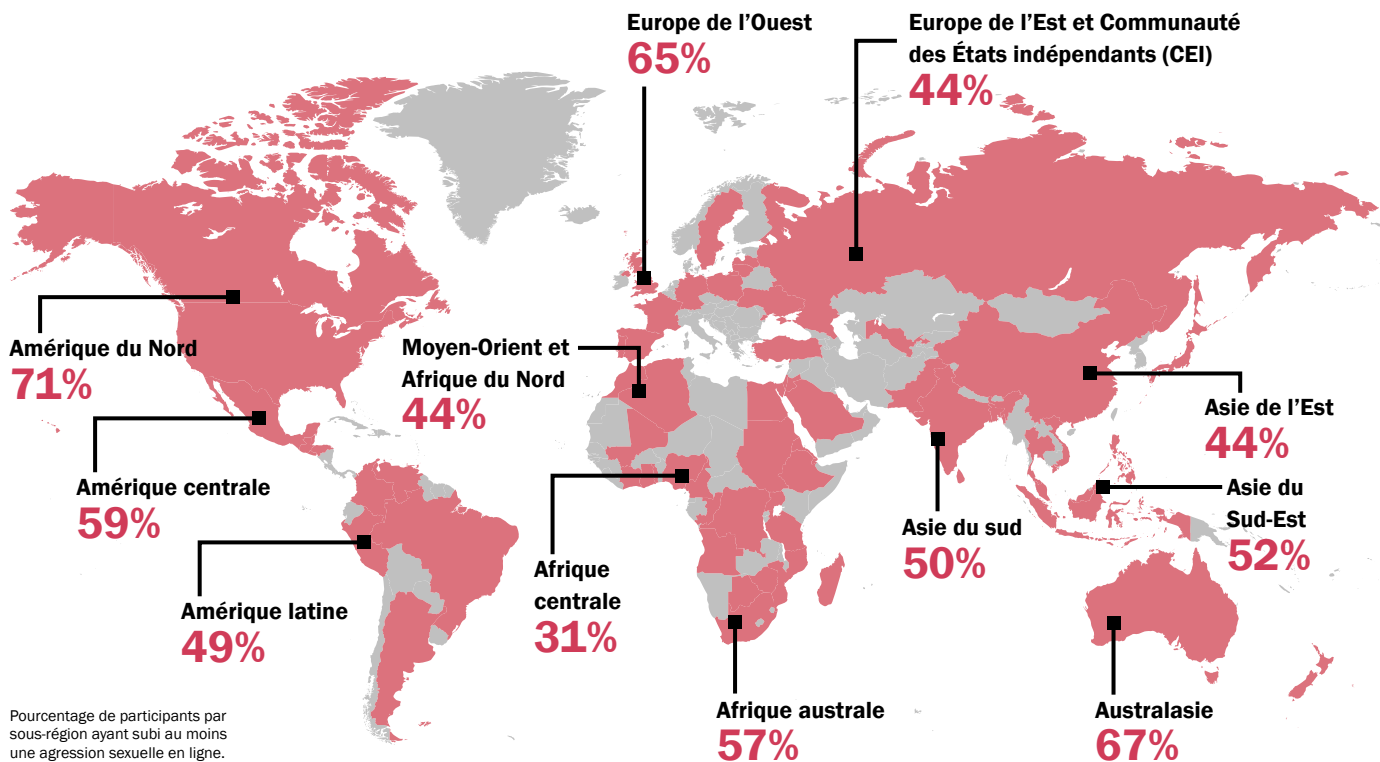
**ont vu des images et/ou vidéos sexuellement explicites d'eux-mêmes partagées par quelqu'un sans leur autorisation**



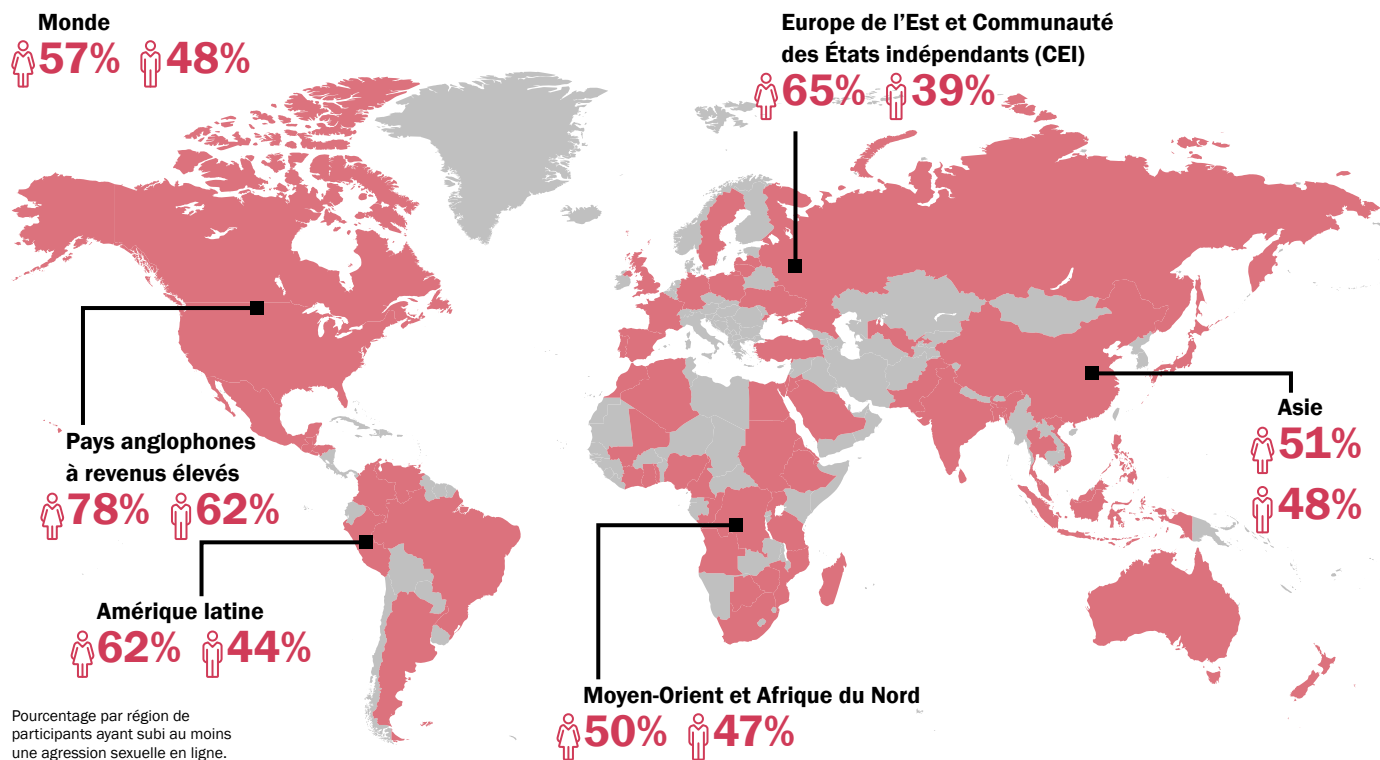
**se sont vu demander de faire quelque chose sexuellement explicite en ligne qui les mettaient mal à l'aise**



**Les agressions sexuelles sur les enfants SE PRODUISENT PARTOUT...**

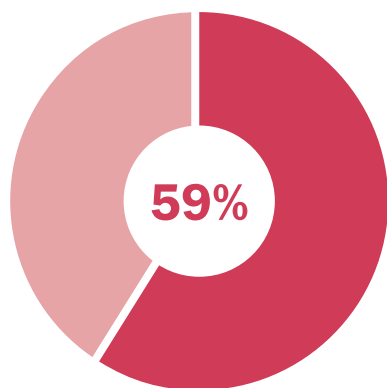


**...et, bien que les filles soient plus à risque, PRÈS DE LA MOITIÉ DES GARÇONS**

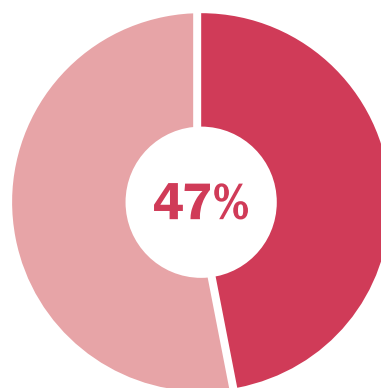


Les participants s'étant identifiés comme transgenres/non-binaires, LGBTQ+ et/ou en situation de handicap montraient **PLUS DE PROBABILITÉ** de subir des agressions sexuelles pendant l'enfance

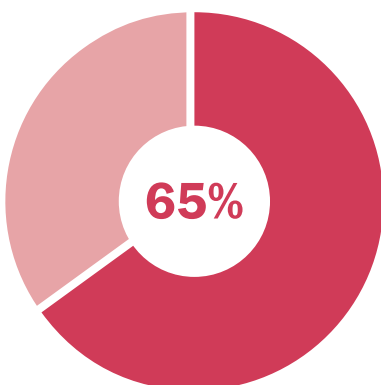
% ayant subi une agression sexuelle en ligne



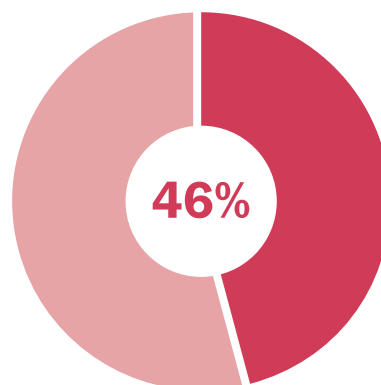
Transgenres/non-binaires



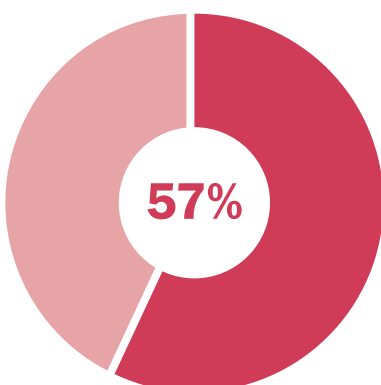
Cisgenres



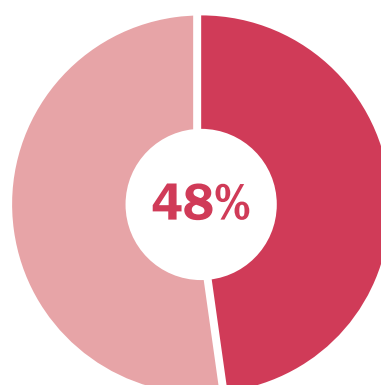
LGBTQ+



Non LGBTQ+



Handicapés

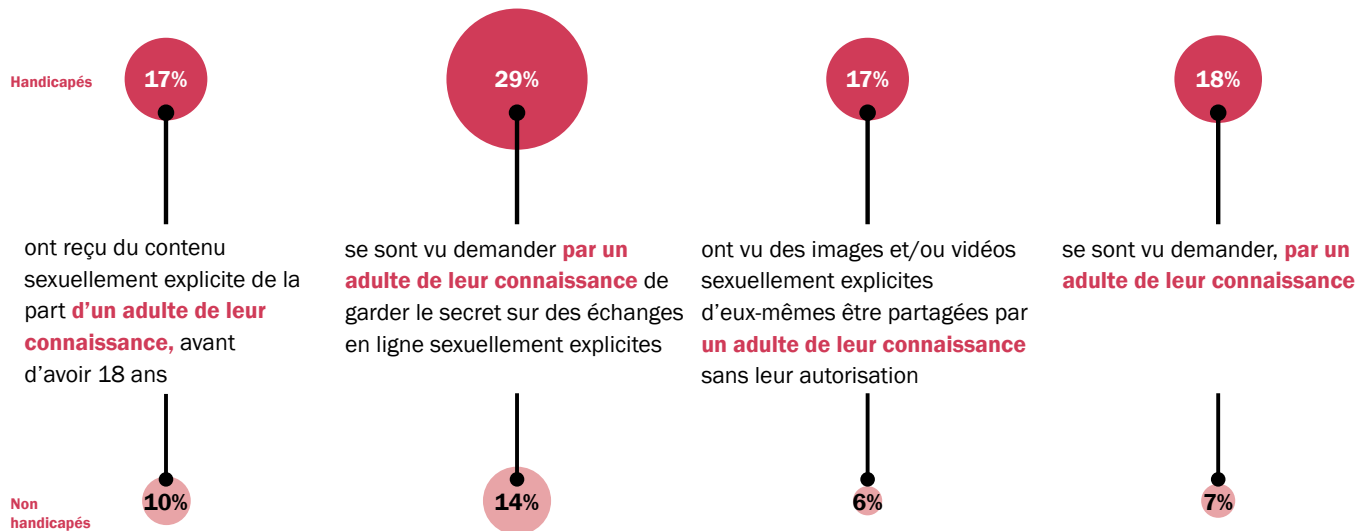


Non handicapés

Pourcentage de participants ayant subi au moins une agression sexuelle en ligne selon des critères auto-identifiés.

Il a été demandé aux participants s'ils s'identifiaient eux-mêmes comme des personnes transgenres/non-binaires, LGBTQ+ et/ou handicapées. Les données figurant dans ce schéma proviennent de l'analyse de la désagrégation de l'échantillon sur la base de ces réponses. Le nombre de participants identifiés selon ces critères dans une région donnée est trop faible pour permettre une analyse précise des écarts géographiques dans les expériences de ces groupes.

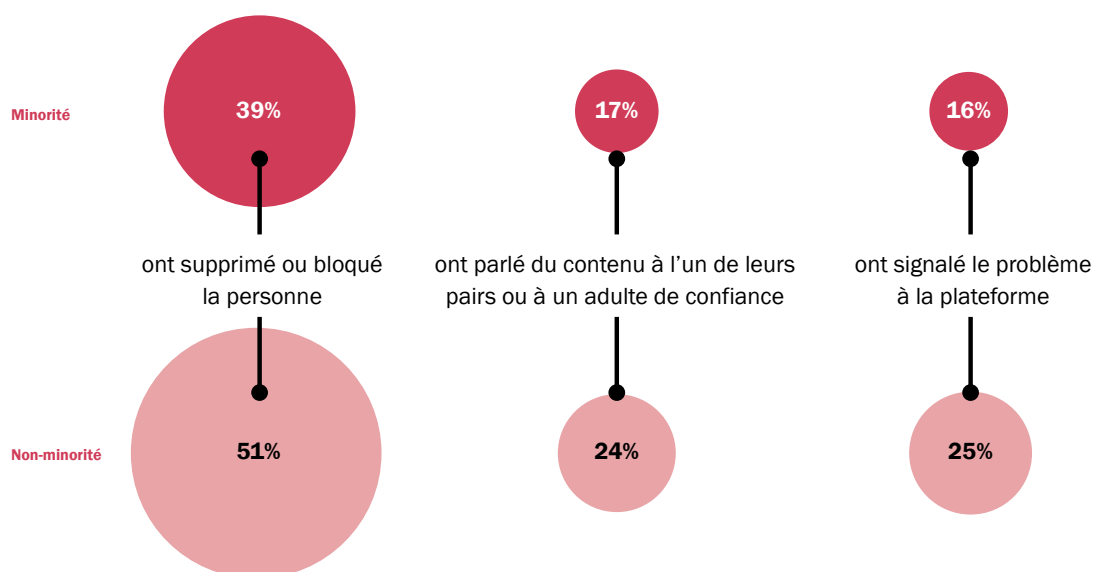
**Les participants s'étant identifiés comme en situation de handicap montraient PLUS DE PROBABILITÉ d'être ciblés par un adulte qu'ils connaissaient.**



Pourcentage de participants (handicapés et non-handicapés) ayant subi une agression sexuelle en ligne par un adulte de leur connaissance.

Le handicap est défini comme une déficience ou un trouble (physique ou mental) qui affecte la capacité du participant à effectuer ses activités quotidiennes.

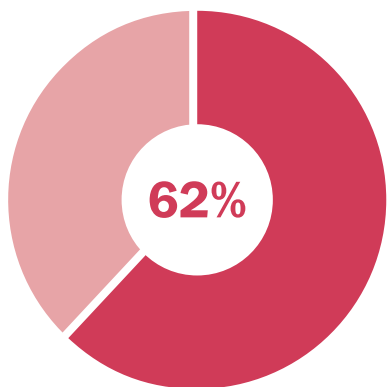
**Les participants s'étant identifiés comme appartenant à des minorités raciales ou ethniques montraient MOINS DE PROBABILITÉ d'agir lorsqu'un adulte de leur connaissance ou non essayait de leur envoyer du contenu sexuellement explicite.**



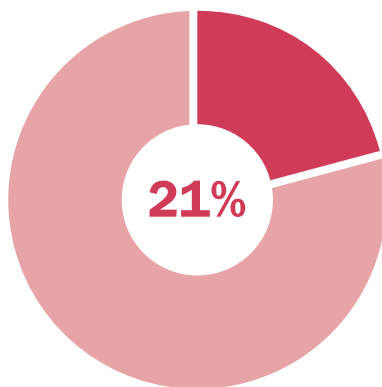
Pourcentage de participants ayant réagi (minorité et non-minorité). La minorité est définie comme une race, une nationalité ou une ethnie différente de celle de la plupart des gens résidant dans le pays du participant.

Les **DEUX TIERS** des participants ayant reçu du contenu sexuellement explicite lorsqu'ils étaient enfants l'avaient reçu via un service de messagerie personnelle, plus généralement sur leur téléphone portable personnel.

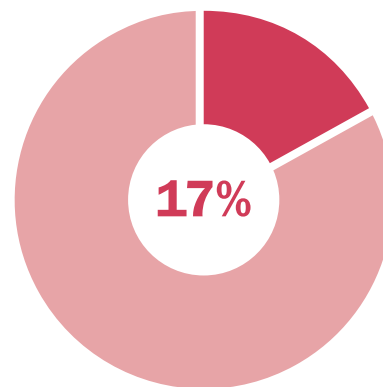
**Appareil** sur lequel les participants ont reçu le contenu



**Leur propre téléphone portable**

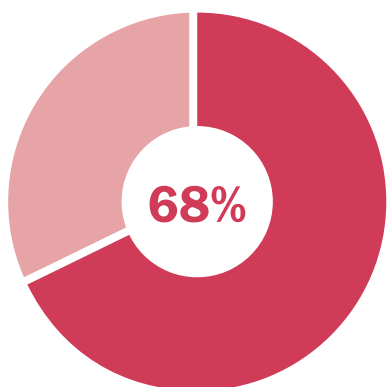


**Le téléphone portable d'un ami**

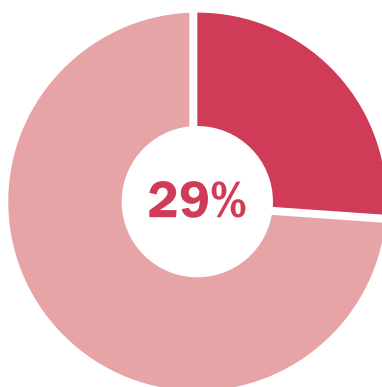


**Leur propre ordinateur de bureau/portable**

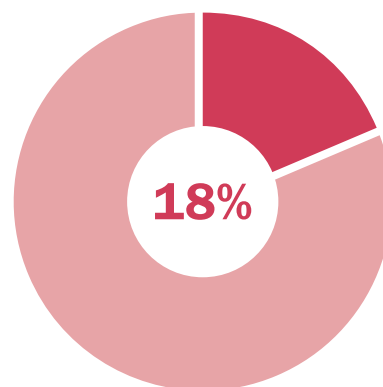
**Plateforme** sur laquelle les participants ont reçu le contenu



**Service de messagerie personnelle**



**Service de partage d'images/vidéos personnelles**



**Forum ouvert d'un réseau social**

## PRINCIPALES CONCLUSIONS

L'ampleur et la portée des agressions sexuelles en ligne envers les enfants aujourd'hui sont probablement différentes. Mais les préoccupations éthiques liées aux enquêtes auprès d'enfants par le biais d'un outil Internet nous ont empêchés de recueillir des données auprès de participants âgés de moins de 18 ans.

Pourquoi les niveaux sont-ils susceptibles d'être différents aujourd'hui?

- La forte croissance de la pénétration d'Internet chez les individus de tous les âges fait qu'un plus grand nombre d'enfants ont un accès régulier à Internet à des âges plus jeunes.
- Un pourcentage plus élevé d'enfants de tous les âges ont accès plus fréquemment aux téléphones mobiles d'adultes et/ou de pairs, et utilisent une plus large sélection de plateformes.
- La COVID-19 a contraint les enfants à passer plus de temps en ligne et a fait que, partout dans le monde, les gens se sont sentis plus isolés.
- Les plateformes numériques sont devenues un moyen courant pour les enfants d'explorer la sexualité avec leurs pairs, mais ces forums d'expression et d'exploration ouvrent également des portes à de nouvelles formes d'abus et d'exploitation.

Des études supplémentaires sont donc nécessaires pour comprendre comment l'univers dynamique d'Internet et des réseaux sociaux/plateformes numériques change la façon dont les enfants interagissent et ce que cela signifie pour leur sécurité contre les menaces en ligne. Notre étude est une première étape dans l'élaboration d'une image globale de ce problème et dans l'identification des points sur lesquels il serait utile d'effectuer d'autres recherches.

## NOTES DE FIN DE DOCUMENT

- i Conformément à la définition d'un enfant dans la Convention relative aux droits de l'enfant, « enfants », dans cette étude, fait référence aux personnes de moins de 18 ans.
- ii « Accès régulier à Internet » désigne une personne qui consulte Internet (et non qui regarde uniquement des pairs, des proches ou d'autres adultes utiliser Internet) au moins une fois par semaine. « Enfants » désigne des personnes âgées de moins de 18 ans. Pour une discussion complète sur la façon dont cette méthode d'échantillonnage est susceptible d'affecter les résultats, voir le document complet.
- iii Un ensemble de comportements nuisibles considérés comme des facteurs de risque d'exploitation et d'abus sexuels potentiels ou réels d'enfants en ligne.
- iv Parmi les personnes ayant répondu à cette enquête, 54% ont subi une ou plusieurs des agressions sexuelles en ligne à propos desquelles elles étaient interrogées.

## MÉTHODOLOGIE

Cette étude est basée sur des données recueillies par le biais d'une enquête en ligne réalisée de mai à juin 2021 auprès de 5 302 jeunes de 18 à 20 ans ayant eu un accès régulier à Internet\* dans leur enfance (quand ils avaient moins de 18 ans).

L'enquête a été menée en 21 langues dans 54 pays, qui ont été regroupés en 12 sous-régions\*\* rassemblant chacune un minimum de 390 participants (pour l'analyse). L'échantillon mondial et l'agrégation régionale ont été utilisés pour étudier les expériences liées au genre et à d'autres caractéristiques démographiques.

### Remarques:

\* « Accès régulier à Internet » désigne une personne qui consulte Internet (et non qui regarde uniquement des pairs, des proches ou d'autres adultes utiliser Internet) au moins une fois par semaine.

\*\* Australasie, Afrique centrale, Amérique centrale, Asie de l'Est, Europe orientale et Communauté des États indépendants, Moyen-Orient et Afrique du Nord, Amérique du Nord, Asie du Sud-est, Afrique australe, Amérique du Sud, Asie du Sud et Europe occidentale.

# 05

# Thèmes

## COVID-19

La COVID-19 a créé un concours parfait de circonstances qui a contribué à l'augmentation de l'exploitation et des abus sexuels envers les enfants dans le monde entier<sup>30</sup>.

Il s'écoulera peut-être des années avant que toute l'ampleur des abus liés à la pandémie ne soit révélée. En attendant, les services en première ligne ont besoin d'un coup de pouce urgent pour soutenir les victimes supplémentaires connues résultant de la COVID-19.

Si les confinements ont pu accélérer les voies menant aux infractions, les effets à long terme de la pandémie menacent de renforcer les facteurs commerciaux des abus.

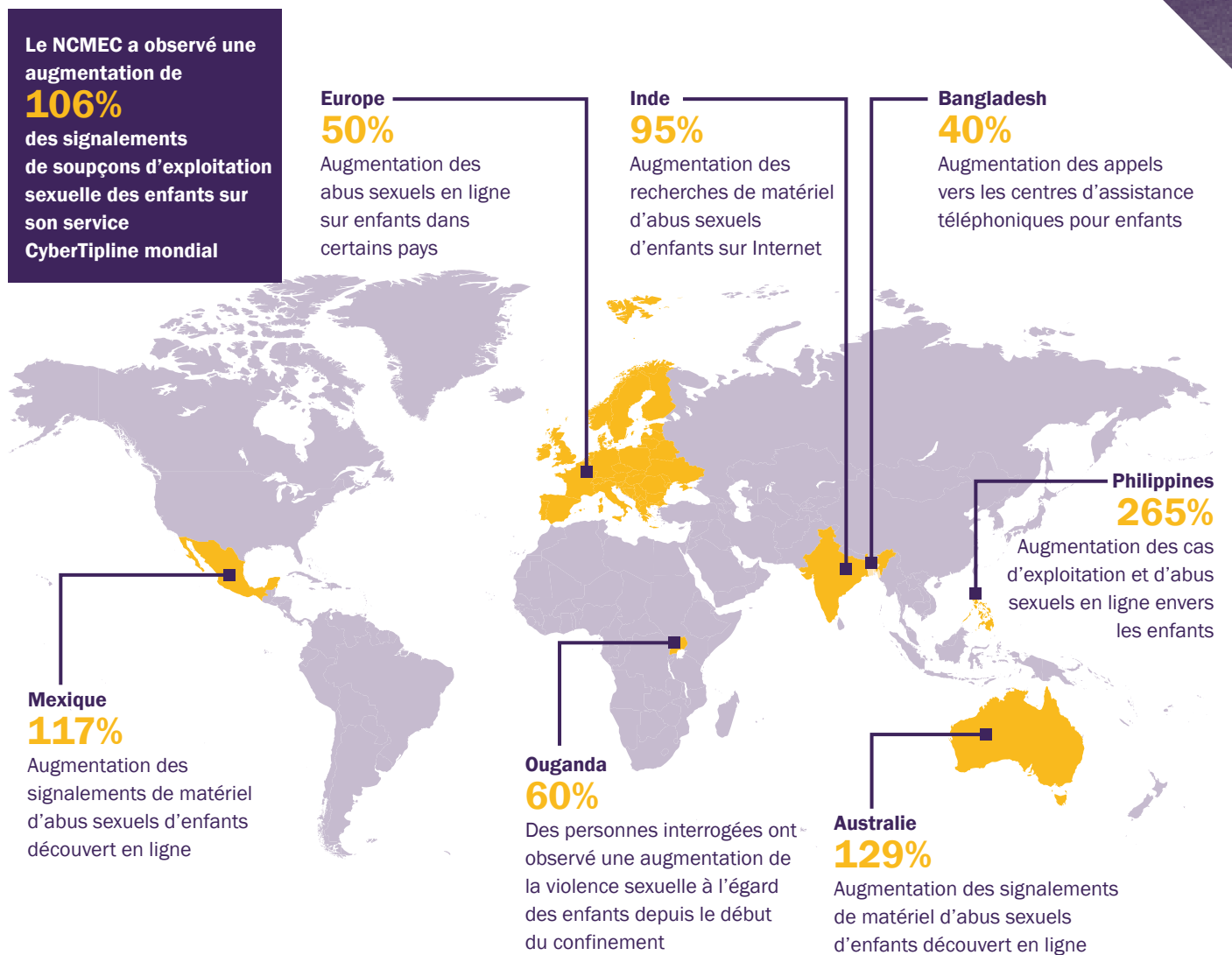
De nombreux pays ont signalé une augmentation de l'exploitation et des abus sexuels envers les enfants pendant la pandémie de COVID-19 (voir figure 5). L'enquête NetClean 2020 sur la répression à l'échelle mondiale montre que la communauté policière s'accorde à dire qu'il y avait une augmentation des tentatives de contact des enfants, des volumes de contenu à caractère sexuel « autoproduit » par les enfants et des activités sur le Dark Web.<sup>31</sup> Certains services de répression prévoient une nouvelle augmentation du volume de matériels d'abus sexuels d'enfants détecté à mesure que davantage de modérateurs reprendront leurs pratiques de travail habituelles.<sup>32</sup>

Pour faire face à cela, les gouvernements devront investir pour renforcer la capacité des services en première ligne et la collaboration du secteur afin de combler les retards dans le signalement.

L'impact réel de la COVID-19 est difficile à distinguer, principalement parce que l'augmentation des signalements d'exploitation et d'abus sexuels envers les enfants pendant la pandémie n'indique pas nécessairement une augmentation équivalente de la criminalité. Les changements dans les pratiques de travail, notamment les équipes mises en télétravail, ont eu une incidence négative sur certains des principaux organismes de recueil des signalements. Dans certains cas, les analystes n'ont pas toujours été en mesure d'évaluer les signalements ou d'exécuter les tâches de modération par rapport aux normes établies, ce qui a entraîné une augmentation des « faux positifs »<sup>33</sup>. Une prise de conscience accrue du problème peut également contribuer à l'augmentation soutenue observée en 2021, car les plateformes d'information et les services de police continuent de mettre en lumière les pics alarmants des taux d'abus signalés.



Figure 5: Augmentation des abus sexuels sur les enfants pendant la COVID-19.<sup>34 35 36 37 38 39 40</sup>



## **En septembre 2020, la fermeture des écoles a touché 827 millions d'élèves dans le monde<sup>41</sup>.**

Au cours de la pandémie, certaines initiatives de prévention de la délinquance ont enregistré une demande accrue de services d'auto-assistance<sup>42,43</sup>. Dès le début, le risque plus élevé d'abus de la part des délinquants a été source d'inquiétude, à cause « du stress, du manque de soutien social positif, des obstacles à la recherche d'aide et de l'augmentation des opportunités » résultant des confinements ; des facteurs « qui sont tous associés au risque de délinquance »<sup>44</sup>. La demande accrue d'auto-assistance montre que ces préoccupations sont confirmées dans une certaine mesure et que les confinements ont peut-être contribué à ouvrir et accélérer les voies de la délinquance chez certaines personnes.

Pour de nombreux délinquants établis, les confinements ont multiplié les occasions de communiquer avec les enfants (en raison de leur plus grande présence en ligne à la maison due à la fermeture des écoles) et ont conféré aux enfants plus d'autonomie sur les réseaux. Dans une enquête mondiale auprès des effectifs impliqués en première ligne dans la protection de l'enfance, 72,8% des participants déclarent avoir constaté au moins une certaine augmentation de l'activité dans les communautés de délinquants en ligne pendant la pandémie.<sup>45</sup>

L'utilisation de « services cachés » (sites Web hébergés dans un réseau proxy afin d'empêcher leur localisation) a également augmenté, ce qui suggère que davantage de délinquants ont appris à masquer leurs activités<sup>46</sup>. En outre, il y a eu une augmentation des abus en ligne sous la forme d'actes par « procuration » de la part d'individus qui, dans d'autres circonstances, auraient pu chercher à abuser en personne des enfants<sup>47</sup>. Ceci est particulièrement préoccupant, car il en résulte un risque accru d'abus commis par diffusion en direct à cause des difficultés économiques causées ou aggravées par la COVID-19. Ainsi que le souligne l'ECPAT: « Comme les familles perdent leurs revenus, en particulier dans les pays du Sud, elles pourraient voir une opportunité dans les "spectacles diffusés en direct" »<sup>48</sup>. Ce n'est pas la moindre des raisons pour laquelle la pandémie a accru la demande de diffusion en direct comme alternative aux abus « physiques »<sup>49</sup>. En ce sens, elle risque également de renforcer à long terme l'intérêt commercial des abus. Il est déjà prouvé que les enfants réagissent aux perspectives économiques difficiles en produisant eux-mêmes du contenu sexuel moyennant paiement<sup>50</sup>.



## **La Banque mondiale estime que le nombre de personnes supplémentaires dans l'extrême pauvreté augmentera de 88 à 115 millions à cause de la pandémie, pour s'élever à 150 millions en 2021<sup>51</sup>.**

Les confinements ont augmenté de nombreux facteurs de risque d'abus. Une intervention en temps utile pour renforcer les services en première ligne surchargés sera essentielle pour venir en aide aux victimes supplémentaires.

Il ne fait aucun doute que les confinements auront réduit le risque pour les enfants de subir des abus à l'extérieur de chez eux (comme dans les établissements). Cependant, pour beaucoup d'autres, les confinements ont créé ou intensifié des vulnérabilités (comme la solitude ou des besoins en santé mentale<sup>52</sup>), augmenté le temps passé en ligne<sup>53</sup> (et de ce fait ont rendu des enfants plus accessibles aux prédateurs<sup>54</sup>) et empêché l'accès aux réseaux de soutien (comme les adultes de confiance, les amis) qui peuvent normalement assurer une protection<sup>55</sup>. Le risque de subir des abus sexuels en ligne pendant la pandémie est probablement plus élevé chez les enfants confrontés à la conjonction de ces facteurs de risque.

Comme indiqué dans la partie *Production de matériels d'abus sexuels d'enfants* du chapitre « Agressions », une part importante des agressions sexuelles sur les enfants est commise par la famille. Les confinements dus à la COVID-19 auront forcé de nombreux enfants à être enfermés à la maison avec leurs agresseurs. La souffrance de ces victimes a probablement été prolongée à cause de l'accès réduit aux canaux habituels de signalement pendant la pandémie. Au Paraguay, les signalements des violences sexuelles infligées aux enfants ont diminué de 50% durant le confinement, mais ont augmenté après l'assouplissement des mesures de confinement, vraisemblablement parce que les victimes (et les adultes de confiance, comme les enseignants ou le personnel de santé) ont pu quitter leur domicile pour signaler les infractions<sup>56</sup>. En Jamaïque, la baisse des signalements officiels d'abus a été contredite par le nombre croissant d'appels téléphoniques vers les lignes d'assistance, ce qui laisse entendre que les enfants étaient dans des situations dans lesquelles les voies habituelles de signalement n'étaient pas accessibles et que « les abus avaient probablement lieu chez eux »<sup>57</sup>.

En Australie, on a noté une diminution des rapports de maltraitance d'enfants pendant la première phase de la pandémie, mais observé un rebond lorsque les restrictions se sont assouplies.<sup>58</sup>

En 2020, des perturbations liées à la pandémie dans les services de protection de l'enfance ont été signalées dans 104 pays, représentant une population totale de 1,8 milliard d'enfants<sup>59</sup>. Dans de nombreuses régions, les capacités policières ont également été touchées. Selon le rapport 2020 de NetClean, la capacité des forces de l'ordre à enquêter sur l'exploitation et les abus sexuels envers les enfants a chuté pendant la pandémie<sup>60</sup>. Interpol a indiqué que la pandémie avait entraîné une réduction du nombre de signalements à la police, des difficultés à faire avancer les enquêtes existantes et une diminution de l'utilisation de la base de données internationale sur l'exploitation sexuelle des enfants.<sup>61</sup>

Comme les pays sortent des confinements et que les victimes signalent tardivement les agressions, l'augmentation du nombre de cas risque d'accroître les retards enregistrés par les services en première ligne. Sans une intervention opportune des gouvernements, les répercussions de la COVID-19 pourraient prolonger les souffrances des enfants et réduire les taux de résolution des cas. C'est ce qui risque de se produire si de nombreux gouvernements à travers le monde réaffectent les fonds des services publics à la stimulation de la reprise économique post-pandémie<sup>62 63</sup>. Une telle action affaiblira la riposte immédiate à la menace et pourrait saper l'éventualité d'une prévention significative à l'avenir. Dans les pays à plus faibles revenus, la situation pourrait s'aggraver si certains suivaient l'exemple de réduction de l'aide publique au développement (APD) décidée par le Royaume-Uni<sup>64</sup>, du fait d'un changement de priorités dans les dépenses. L'impact de ces coupes budgétaires pourrait se traduire par un accroissement des répercussions à long terme des futures crises sanitaires, y compris le développement de l'exploitation et la multiplication des abus sexuels envers les enfants.

# 05

# Thèmes

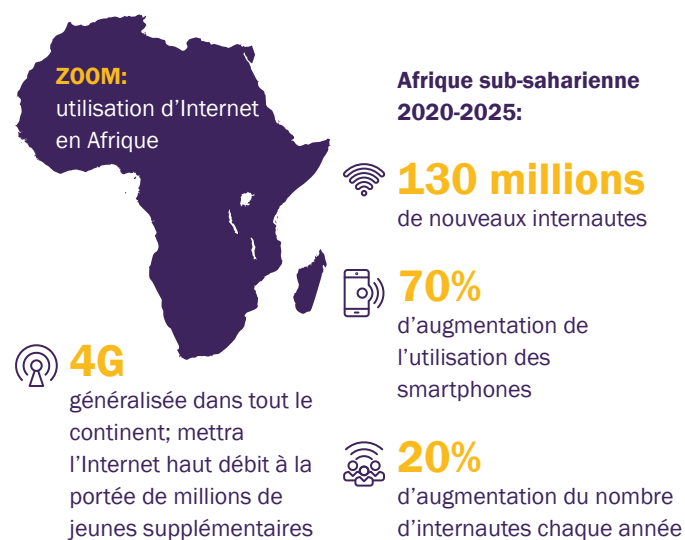
## Technologie

### Le rythme de l'évolution technologique continue de compliquer la riposte à l'exploitation et aux abus sexuels en ligne envers les enfants.

Toutefois, ces dernières années, les technologies de sécurité en ligne ont considérablement évolué. Avec une utilisation généralisée, ces outils et techniques pourraient permettre le changement radical requis dans la riposte mondiale à la menace.

En 1995, moins de 1% de la population mondiale était active sur Internet<sup>65</sup>. Aujourd'hui, ce chiffre est passé à 59,5%<sup>66</sup>. La vitesse de téléchargement moyenne augmente également à l'échelle internationale<sup>67</sup> et le nombre d'appareils mobiles actifs dans le monde devrait atteindre 17,62 milliards d'ici 2024, soit 3,7 milliards d'appareils en plus qu'en 2020<sup>68</sup>. Dans certaines parties du globe, comme le continent africain, ces changements se produisent à un rythme nettement accéléré (voir figure 6). Les moins de 18 ans représentent désormais un tiers des utilisateurs de la planète<sup>69</sup>.

Figure 6: Utilisation d'Internet en Afrique<sup>70 71 72</sup>



Comme l'ont souligné les Nations Unies dans leur Observation générale n° 25 (voir *Glossaire*), l'environnement numérique facilite l'accès à un ensemble de droits des enfants, car un nombre sans cesse grandissant de fonctions sociétales dépendent des technologies numériques. Les opportunités éducatives de ces technologies ont le potentiel d'être particulièrement transformatrices. L'augmentation du nombre d'appareils mobiles a été saluée comme une excellente occasion d'atteindre la population mondiale des filles qui représente « les deux tiers des enfants d'âge primaire non scolarisés dans le monde »<sup>73</sup>. Pour les enfants, les avantages sociaux de la connexion sont également importants. Dans l'enquête européenne Kids Online 2020, la majorité des participants « affirment qu'il est plus facile d'être soi-même en ligne, au moins de temps en temps »<sup>74</sup>. Cela peut fortement transformer les jeunes dont la liberté d'expression est limitée par ailleurs (par exemple, à cause d'un handicap ou d'une déficience, ou parce qu'ils résident dans un contexte socio-environnemental restrictif).<sup>75</sup>

**Mais pour certains enfants, les avantages de cette connectivité sont actuellement battus en brèche par l'expérience de comportements destructeurs et d'abus sexuels avec toutes les conséquences négatives que cela implique.**

Les faits montrent qu'être en ligne expose une partie d'entre eux à des interactions sexuelles<sup>76</sup> et des images sexuelles<sup>77 78</sup>. Bien que certains enfants (plus âgés) puissent percevoir cela comme des opportunités d'explorer leur identité sexuelle, chez d'autres, notamment les plus jeunes, cela risque d'entraîner un impact négatif sur le développement<sup>79</sup>. Comme il est expliqué dans la partie *Recherche et/ou consultation de matériels d'abus sexuels d'enfants* du chapitre « Agressions », l'exposition régulière à la pornographie est associée au développement de comportements sexuels malveillants (voir *Glossaire*) chez les adolescents.<sup>80 81</sup>



L'étude d'Economist Impact, commanditée en parallèle de ce rapport, révèle que 62% des participants ayant déclaré avoir reçu du contenu sexuellement explicite l'avaient reçu sur leur appareil mobile. Dans de nombreux pays, les smartphones sont aujourd'hui le moyen préféré des enfants pour se connecter.<sup>82 83</sup>

Mais l'accès accru à Internet via les appareils mobiles connectés contribue au sentiment d'être piégé chez les enfants qui deviennent victimes d'abus, car les délinquants semblent s'infiltrer dans tous les aspects de leur vie quotidienne<sup>84</sup>. L'enquête menée par Thorn en 2021 auprès de jeunes Américains révèle que de nombreux enfants réagissent aux interactions sexuelles malveillantes en ligne en minimisant leur impact et en ne les divulguant pas, autant de tactiques susceptibles d'amplifier et/ou d'étendre les dommages causés.<sup>85</sup>

Cependant, il existe des signes positifs montrant que des défenseurs, notamment les enfants et les jeunes eux-mêmes, commencent à remettre en cause l'apparente « normalisation » des agressions sexuelles. Au Royaume-Uni au début de l'année 2021, les révélations sur la « culture du viol » dans les écoles ont incité les adolescents à partager leurs expériences de harcèlement sexuel dans le cadre du mouvement « Everyone Invited ». Cette initiative a depuis rassemblé plus de 50 000 témoignages et généré un mouvement similaire aux États-Unis<sup>86 87 88</sup>. Bien qu'Internet ait joué un rôle dans le développement de l'exploitation et la multiplication des abus sexuels, il offre également aux jeunes une plateforme pour exiger un changement.<sup>89</sup>

**La plupart des services de forces de l'ordre manquent des capacités nécessaires pour enquêter sur l'exploitation sexuelle des enfants en ligne.**

Les délinquants disposant d'un savoir-faire technique minimum peuvent même compliquer la détection des agressions en utilisant des solutions d'anonymisation telles que Tor et les réseaux privés virtuels (VPN), qui sont maintenant courants et intégrés par défaut dans certains navigateurs<sup>90</sup>.

L'utilisation du chiffrement progresse également (voir *Réglementation, coopération volontaire et transparence* dans le chapitre « Agressions »). L'effet global est un obstacle significatif aux enquêtes du fait des technologies faciles d'emploi. Les délinquants du Dark Web posent une série de défis différents. Les plus avancés d'entre eux sur le plan technologique exploitent les possibilités offertes par de nouveaux outils pour commettre leurs agressions et échapper à la détection.

Le nombre d'appareils mobiles actifs à travers le monde devrait atteindre le chiffre de

**17,62 MILLIARDS**

d'ici 2024

D'après l'étude d'Economist Impact commanditée parallèlement à ce rapport, sur l'ensemble des participants à l'enquête ayant déclaré avoir reçu du contenu explicitement sexuel,

**62%**

l'avaient reçu sur leur téléphone portable.

# Les délinquants sur le Dark Web recherchent de nouveaux outils pour faciliter l'exploitation.



Les agresseurs sur le Dark Web ont une approche de plus en plus sophistiquée et sont à l'aise avec la technologie de pointe utilisée pour créer et distribuer du matériels d'abus sexuels d'enfants. Pour compliquer la situation, une nouvelle génération technophile de délinquants sur le Dark Web utilise et promeut des techniques et services de sécurité avancés pour échapper à la détection.

Comme ces délinquants cherchent en permanence de nouvelles options et solutions en ligne pour faciliter l'exploitation des enfants, il est encore plus difficile pour les forces de l'ordre d'enquêter sur leurs actes et de les poursuivre. Il est inquiétant de constater que leur boîte à outils opérationnelle évolue et s'enrichit au rythme actuel de l'innovation technologique en ligne.

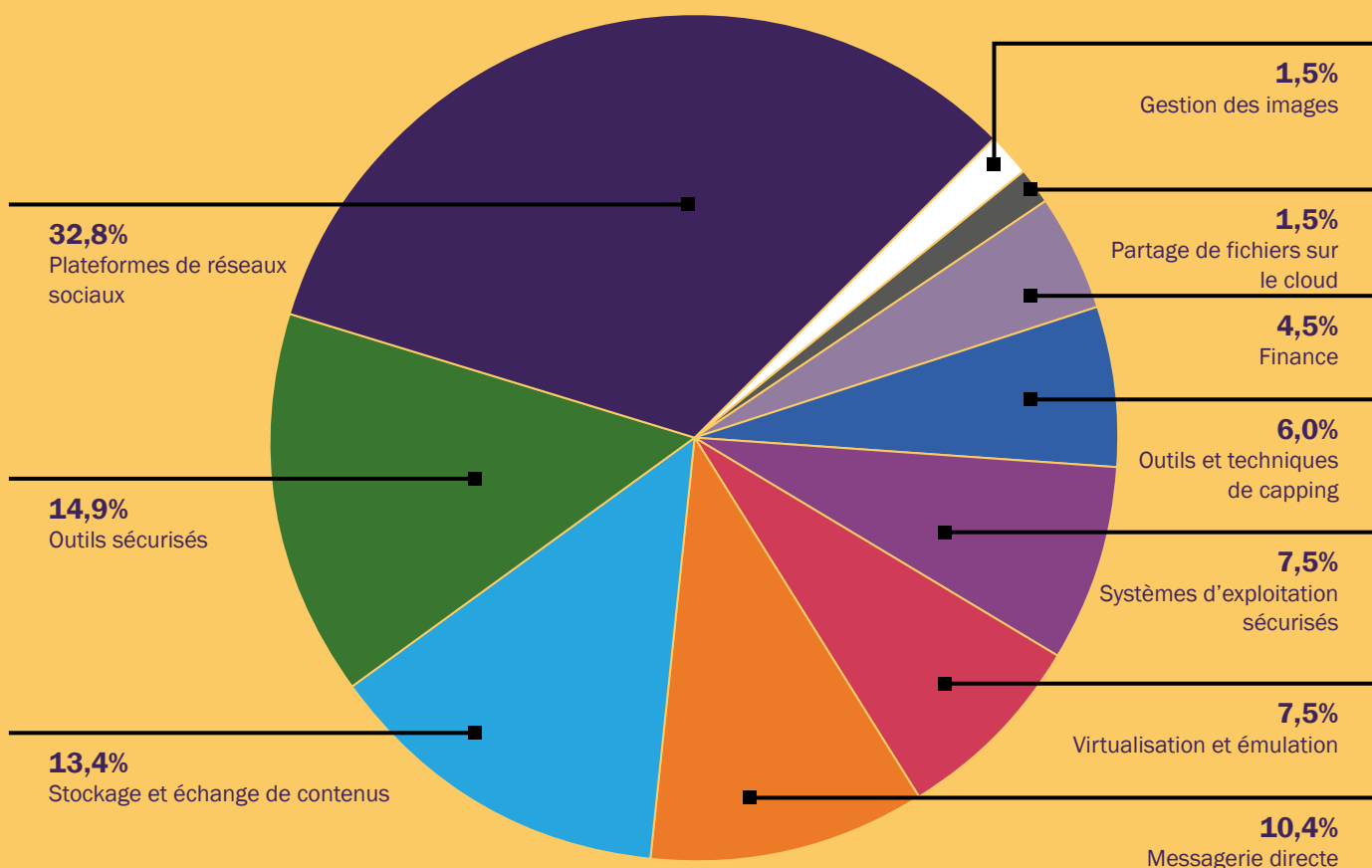
Les analystes de Crisp ont pu mesurer leur niveau d'intérêt pour les sujets technologiques en examinant de près les conversations

tenues dans différents forums de délinquants sur le Dark Web en février 2021.

Parmi les « thèmes technologiques » abordés, près d'un tiers concernaient des plateformes sur lesquelles les délinquants pouvaient chercher à dialoguer avec des enfants ou des utilisateurs vulnérables, ainsi que des discussions plus larges sur « les techniques de dissimulation » (voir *Glossaire*). Ce qui est plus préoccupant encore, c'est que plus des deux tiers des discussions portaient sur des sujets tels que les outils techniques des messageries directes, l'échange de fonds ou la façon d'acquérir et de stocker du contenu en toute sécurité, que ce soit localement ou sur le cloud. Tout cela peut rendre plus difficiles l'identification et la poursuite des délinquants.

Pour consulter les définitions sur les thèmes technologiques, veuillez consulter le *Glossaire*.

Figure 7: Thèmes technologiques abordés dans les forums de délinquants sur le Dark Web.



Comme d'autres infractions liées à Internet, l'exploitation et les abus sexuels en ligne envers les enfants posent des problèmes fondamentaux à la plupart des services de police en matière d'enquête: il s'agit le plus souvent de capacités numériques limitées, d'un personnel insuffisamment qualifié et d'un manque d'accès aux outils pour accélérer certains aspects des processus d'enquête. Le Sri Lanka a récemment signalé un manque de personnel technique dans les unités d'enquête<sup>91</sup>, tandis que la police thaïlandaise a déclaré avoir besoin de davantage de ressources formées aux enquêtes sur le Dark Web et aux paiements en cryptomonnaie liés à la criminalité.<sup>92</sup>

Certains pays répondent à ce problème en regroupant l'exploitation et les abus sexuels en ligne envers les enfants dans les attributions des unités de cybercriminalité, où ces affaires se disputent l'attention avec des crimes de grande ampleur, souvent complexes, comme la fraude. Dans certains endroits, la coopération avec les prestataires de services en ligne est également à la traîne. Selon Interpol, le non-respect des mandats d'arrêt est un défi mondial majeur<sup>93</sup>. Les différences entre les politiques de conservation des données dans les entreprises peuvent également compliquer la collecte de preuves pour les services de police.

La cause fondamentale de la plupart de ces problèmes est l'insuffisance chronique du financement des services de police. Il est urgent d'investir dans le renforcement des capacités d'enquête numérique des forces de l'ordre dans le monde entier, ainsi que dans le développement et l'amélioration des mécanismes de collaboration indispensables à une lutte efficace contre les infractions transfrontalières et technologiquement sophistiquées.<sup>94</sup>

**Certains cadres législatifs ne sont toujours pas adaptés à l'ère numérique. Ces lacunes risquent de créer un sentiment d'impunité autour des abus sexuels sur les enfants commis en ligne.**

Certes, au cours des dernières décennies, les approches législatives relatives aux agressions sexuelles envers les enfants ont été plus cohérentes, catalysées par des instruments internationaux comme la Convention de Lanzarote (voir *Glossaire*). Toutefois, des différences subsistent. Depuis 2006, l'International Centre for Missing and Exploited Children procède régulièrement à un examen des législations relatives aux agressions sexuelles sur les enfants dans les 196 pays membres d'Interpol. La première enquête a révélé que la législation était « suffisante » dans 27 pays seulement. La dernière édition (2018) révèle que 71 pays en sont encore à définir le matériels d'abus sexuels d'enfants, et que 32 seulement exigent des prestataires de services Internet qu'ils signalent ces infractions.<sup>95</sup>

Le rôle de la technologie dans les délits d'exploitation et d'abus sexuels envers les enfants débouche sur une série de complexités législatives particulières.

Les différences dans le traitement des abus « en ligne » par rapport à celui des abus physiques sont fréquentes et citées comme une raison pour laquelle les délinquants sur Internet semblent opérer en toute impunité. Un examen des cas par l'organisation caritative International Justice Mission (IJM) souligne que seuls l'Écosse, le Canada, l'Australie et la Suède punissent les agressions en ligne « à parité avec les infractions physiques »<sup>96</sup>. De nombreux pays ne disposent pas non plus d'une définition juridique de l'utilisation de contenus d'abus sexuels d'enfants non photographiques<sup>97-98</sup>. L'impact de cette lacune pourrait augmenter à mesure que les délinquants diversifient leurs méthodes de production à l'aide de techniques comme les images de synthèse (voir *Production de matériels d'abus sexuels d'enfants* dans le chapitre « Agressions »). Ces lacunes risquent de créer un sentiment d'impunité et de favoriser les agressions, d'autant plus qu'il semblerait que les délinquants ciblent volontairement les enfants dans les pays où les mesures sont moins strictes.<sup>99</sup>

**Cependant, la technologie existe désormais aussi pour protéger les enfants et poursuivre les délinquants. Sous réserve d'une large adoption, les outils et techniques de sécurité en ligne ont le potentiel de transformer la riposte mondiale à la menace.**

Ces dernières années, il y a eu d'importants progrès dans les technologies de sécurité en ligne. Parmi les principaux exemples, citons:

- Les outils de détection des sollicitations en ligne et les fonctions d'intégration de la sécurité à la conception (« Safety by design ») qui réduisent le champ des possibilités des délinquants et favorisent les comportements sûrs en ligne (voir *Sollicitations d'enfants en ligne à des fins d'exploitation et d'abus sexuels* dans le chapitre « Agressions »).
- Les mécanismes de dissuasion qui interrompent le parcours vers la criminalité (voir *Recherche et/ou consultation de matériels d'abus sexuels d'enfants* dans le chapitre « Agressions »).
- Les solutions de correspondance de hachage (voir *Glossaire*) pour détecter et supprimer le matériels d'abus sexuels d'enfants connu, et l'utilisation de classificateurs pour déceler les contenus de première génération (voir *Partage et/ou stockage de matériels d'abus sexuels d'enfants* dans le chapitre « Agressions »).

Le développement du secteur des technologies de sécurité a joué un rôle central dans le développement de nombre de ces technologies. Rien qu'au Royaume-Uni, où les sociétés de technologies de sécurité détiennent ensemble 25% de la part de marché mondiale, le secteur a connu un taux de croissance annuel estimé à 35% depuis 2016<sup>100</sup> et devrait atteindre 1 milliard de livres sterling de chiffre d'affaires d'ici 2024 (voir figure 8 ci-dessous)<sup>101</sup>. Plus de la moitié des entreprises britanniques (52%) ont une présence internationale établie.<sup>102</sup>

En réduisant les possibilités pour les délinquants et en améliorant la protection offerte aux enfants, les technologies de sécurité en ligne ont le potentiel de dynamiser la riposte mondiale à l'exploitation et aux abus sexuels en ligne envers les enfants. Ceci sans tenir compte de l'impact possible des outils et des techniques encore en développement, notamment:

- L'amélioration de la reconnaissance faciale, qui pourrait accélérer l'identification des enfants victimes de tels actes.<sup>103</sup>
- Les analyses prédictives qui permettent d'intervenir à un stade précoce et qui sont déjà utilisées par certaines autorités pour identifier les enfants à haut risque d'être agressés.<sup>104</sup>
- Les outils capables de collecter des métadonnées (voir *Glossaire*) pour détecter du contenu potentiellement d'abus sexuels d'enfants, même si le contenu lui-même n'est pas décelable.<sup>105</sup>
- Les techniques de capture d'empreinte des appareils photo, utilisées pour attribuer des photos et/ou des vidéos à un appareil spécifique. Dans certains pays, ces techniques sont déjà utilisées pour rationaliser et renforcer les poursuites.<sup>107</sup>.

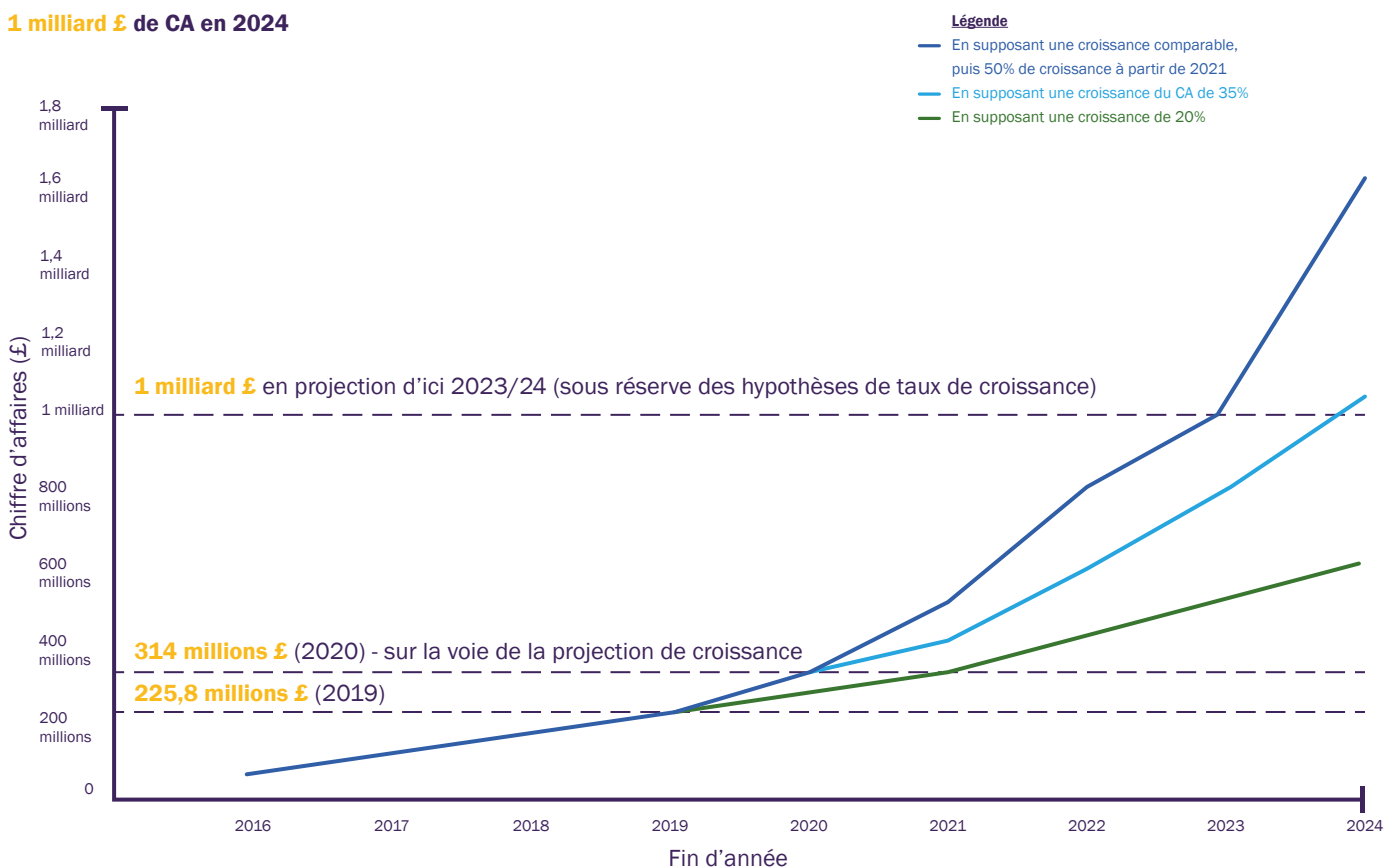
## QU'ENTEND-ON PAR TECHNOLOGIE DE SÉCURITÉ (« SAFETY TECH »)?



Les fournisseurs de technologies de sécurité développent des technologies ou solutions destinées à favoriser les expériences en ligne plus sûres et à protéger les utilisateurs contre les contenus, contacts ou comportements malveillants<sup>106</sup>.

Figure 8: Tableau des prévisions de croissance du secteur britannique des technologies de sécurité, reproduit avec la permission du ministère britannique du Numérique, des Médias, de la Culture et des Sports<sup>108</sup>.

### 1 milliard £ de CA en 2024



## APPLE: UNE PROTECTION ÉTENDUE POUR LES ENFANTS

Apple envisage de lancer des dispositifs de sécurité supplémentaires pour protéger les enfants aux États-Unis. Parmi ceux-ci, citons:

- Des nouveaux outils intégrés aux appareils qui préviennent les enfants et, dans le cas des moins de 13 ans, leurs parents ou tuteurs lorsqu'ils reçoivent ou envoient des photos sexuellement explicites, si les parents ou tuteurs ont choisi d'être avertis.
- Des mises à jour de Siri et de Search pour aider les utilisateurs impliqués dans des situations sexuellement malveillantes en ligne et hors ligne, et aussi pour intervenir lorsque des utilisateurs tentent de trouver du matériel d'abus sexuels d'enfants et leur fournir les ressources et avertissements nécessaires afin de prévenir les abus.
- L'utilisation du nouvel outil NeuralHash pour identifier le matériel d'abus sexuels d'enfants « connu » stocké dans la bibliothèque de photos iCloud, en comparant son contenu à celui d'une base de données de hachages d'images d'abus sexuels sur les enfants. Si la correspondance de hachage dépasse un certain seuil, ceci sera examiné par un être humain pour confirmation avant l'envoi d'un signalement au NCMEC. Le processus de mise en correspondance est alimenté par des technologies de chiffrement appelées Private Set Intersection et Threshold Secret Sharing, qui déterminent s'il existe une correspondance sans révéler le résultat, à moins que le seuil ne soit atteint. Apple ne peut rien apprendre sur le compte d'un utilisateur sauf si une collection d'images correspondant à un contenu d'abus sexuels d'enfants « connu » a été détectée.

Fondamentalement, ces fonctionnalités pourraient être compatibles avec le service iMessaging chiffré d'Apple et démontrer la possibilité continue de contrecarrer la menace d'exploitation et d'abus sexuels envers les enfants, même dans des environnements chiffrés, en adoptant des technologies côté serveur et au niveau des appareils, tout en préservant la confidentialité des données.

## GLOBAL PARTNERSHIP TO END VIOLENCE AGAINST CHILDREN: SAFE ONLINE FUND

L'initiative Safe Online fait partie du Global Partnership to End Violence Against Children et investit dans des interventions programmatiques, la production de preuves et l'innovation technologique pour lutter contre les abus sexuels sur les enfants en ligne. Depuis 2017, Safe Online a investi un total de 48 millions de dollars dans 60 projets. En 2020, 10 millions de dollars ont été dépensés dans la conception et l'intégration de solutions technologiques.

Outre les investissements financiers destinés à renforcer la riposte aux violences sexuelles sur les enfants en ligne, l'initiative Safe Online du Global Partnership to End Violence Against Children encourage la création de contenus éducatifs et la collaboration afin d'optimiser l'utilisation des ressources collectives et d'assurer que les investissements ont un impact efficace.

Safe Online joue un rôle essentiel dans la promotion et le pilotage d'une action collaborative visant à aligner les efforts mondiaux, régionaux et nationaux pour lutter contre les agressions en ligne envers les enfants.

Cette vision repose sur l'augmentation des investissements de la part des gouvernements et des entreprises du secteur privé pour développer des solutions de protection des enfants. Comme le souligne l'organisme End Violence Partnership, l'insuffisance des investissements demeure le plus grand obstacle à une réponse efficace à l'exploitation et aux abus sexuels en ligne envers les enfants<sup>109</sup>. Une utilisation large et cohérente des technologies sera essentielle pour éviter que les délinquants n'orientent simplement les enfants vers des plateformes dépourvues de mécanismes de sécurité intégrés.

En parallèle de cette adoption, un alignement juridique international de l'utilisation de ces technologies deviendra de plus en plus essentiel<sup>110</sup>, en tenant compte des considérations éthiques et de protection de la confidentialité soulevées par beaucoup. Les gouvernements doivent consulter attentivement les entreprises pour élaborer des cadres juridiques permettant une innovation responsable qui place les droits des enfants au centre de la conception et du déploiement de la technologie. Ils doivent inclure la protection du droit des enfants à la vie privée, des explications « adaptées à l'âge » et la non-discrimination dans l'application des algorithmes d'intelligence artificielle<sup>111</sup>. Les mécanismes de protection des jeunes enfants méritent une attention particulière pour éviter de les priver d'opportunités en raison des risques perçus, notamment parce qu'une faible documentation numérique pourrait en fin de compte les rendre plus vulnérables aux abus<sup>112</sup>.

# 05

## Thèmes

### Règlementation, coopération volontaire et transparence.

#### Le rythme de l'évolution technologique continue de compliquer la riposte à l'exploitation et aux abus sexuels en ligne envers les enfants.

Le développement de l'exploitation et la multiplication des abus sexuels en ligne envers les enfants ont alimenté le débat sur la réglementation d'Internet ces dernières années.

À mesure qu'un nombre grandissant de pays s'orientent vers la réglementation des prestataires de services en ligne, la coopération volontaire et la transparence continueront d'être essentielles pour consolider la riposte mondiale.

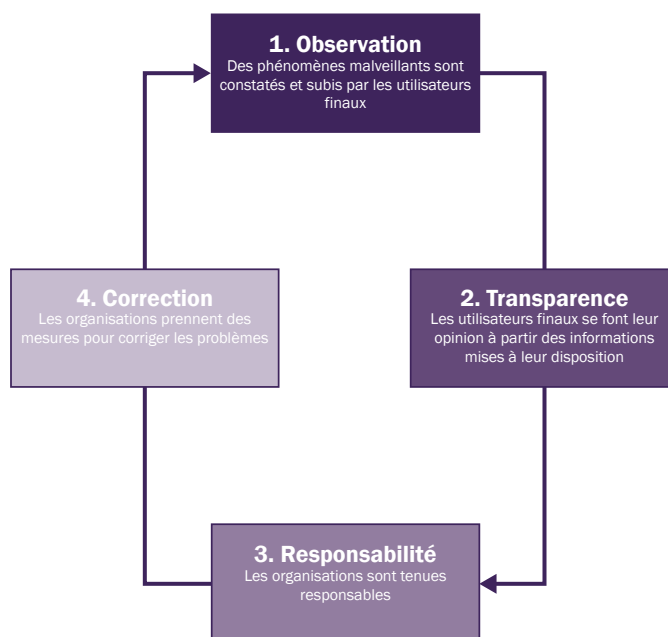
La réglementation vise à établir des normes pour équilibrer la confidentialité et la sécurité des utilisateurs afin de permettre une approche plus cohérente dans la lutte contre les agressions en ligne.

Au cours des trois dernières années, la réglementation des services numériques et de la sécurité en ligne a connu un élan considérable. Parmi les premiers pays à rechercher une solution législative figurent l'Australie, l'Allemagne, le Royaume-Uni, les pays de l'Union européenne et l'Irlande (voir figure 10).

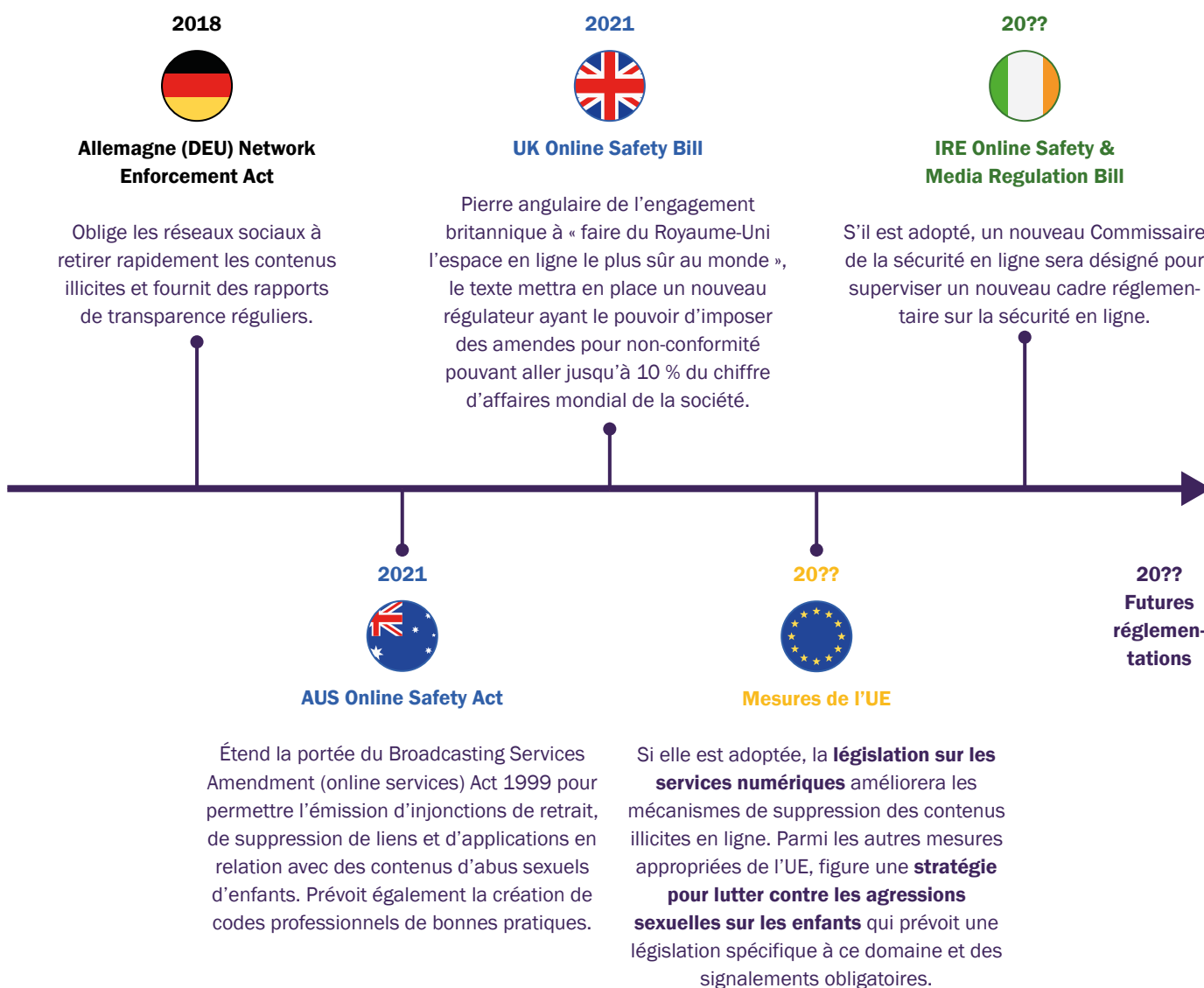
Les systèmes réglementaires efficaces suivent un cycle cohérent en 4 étapes (voir figure 9).

La réglementation des agressions en ligne est relativement embryonnaire par rapport à celle d'autres secteurs, comme l'aéronautique, l'agroalimentaire et les services financiers. La transparence est limitée, la responsabilité est volontaire et les mesures correctives ne sont pas homogènes. Pourtant, la sensibilisation croissante aux agressions crée une pression internationale grandissante en faveur d'une transparence, de normes de responsabilité et de mesures correctives homogènes à mettre en œuvre via la législation et la réglementation.

Figure 9: Les étapes d'un cycle réglementaire efficace.







Dans le monde physique, des cadres juridiques aident les autorités et les entreprises à équilibrer vie privée et sécurité individuelle. Mais dans le monde en ligne, ces normes ne font qu'émerger. En précisant les responsabilités des prestataires de services en ligne, la réglementation pourrait établir un équilibre plus cohérent qui protège mieux les utilisateurs d'Internet contre les agressions, en particulier les enfants<sup>119</sup>.

**L'utilisation croissante du chiffrement de bout en bout (end-to-end encryption ou E2EE en anglais) est un bel exemple du risque d'une absence de normes de sécurité en ligne uniformes et plaide en faveur de la réglementation.**

Le cryptage et l'E2EE ont gagné en popularité ces dernières années, le public ayant une conscience accrue de la protection de ses données et de sa vie privée en ligne. Le chiffrement de bout en bout est l'un des systèmes de protection de la vie privée les plus efficaces qui soient. Le rapporteur spécial de l'ONU sur la liberté d'expression l'a décrit comme « l'élément le plus fondamental de la sécurité numérique dans les applications de messagerie », soulignant la protection qu'il peut offrir aux minorités encourant « un risque grave de persécution et de violations des droits humains »<sup>120</sup>. Le chiffrement de bout en bout est déjà intégré à certains services de messagerie et plusieurs grandes plateformes ont annoncé des projets de mise en œuvre<sup>121</sup> ou d'extension de cette fonctionnalité<sup>122</sup>.

**QU'EST-CE QUE LE CHIFFREMENT DE BOUT EN BOUT?**

Il s'agit d'une forme de chiffrement dans laquelle le contenu de chaque message est visible uniquement par l'expéditeur et le destinataire. Le déchiffrement du message nécessite l'échange d'une clé de déchiffrement privée entre les correspondants de sorte que, même si le message est intercepté, il ne peut être ni visualisé ni surveillé par le prestataire de services, les services de répression ou tout autre tiers<sup>123</sup>.

Cependant, il ruine les efforts de lutte contre l'exploitation et les abus sexuels en ligne envers les enfants. En effet, la plupart des technologies de détection (par exemple, correspondance de hachage, algorithmes de détection des sollicitations, classificateurs pour identifier le matériels d'abus sexuels d'enfants) ne sont pas facilement utilisables dans les environnements E2EE.

Les désaccords en Europe sur l'utilisation des technologies de détection automatisée ont donné par inadvertance un aperçu des conséquences probables de l'impossibilité de déployer ces outils. Le NCMEC a constaté une baisse de 58% des signalements sur CyberTipline au sein de l'UE lorsque l'utilisation de ce service a été interrompue par certaines entreprises en décembre 2020, afin de se conformer à la Directive européenne sur la protection de la vie privée<sup>124 125</sup>. Une dérogation temporaire à la législation a été acceptée en mai 2021<sup>126</sup>, mais elle ne permet de rétablir la détection que pour une durée de trois ans. Comme le souligne l'ECPAT<sup>127</sup>, une réponse législative à long terme est nécessaire pour résoudre le problème. Il est à espérer que l'adoption par l'UE d'une nouvelle stratégie concernant les droits de l'enfant<sup>128</sup>, ainsi que les efforts pour renforcer la lutte contre les violences sexuelles sur les enfants en ligne<sup>129</sup>, ouvriront la voie à une solution.

En dissimulant l'ampleur de l'exploitation et des abus sexuels envers les enfants décelables en ligne<sup>130</sup>, l'utilisation croissante du chiffrement de bout en bout fait qu'il devient difficile de défendre une hausse des investissements pour lutter contre la menace<sup>131</sup>. Elle risque également de compliquer les enquêtes menées par les forces de l'ordre, dans la mesure où les demandes de mandats pour accéder aux appareils des suspects (afin d'obtenir les preuves de leurs actes) ne permettraient plus de citer le contenu des communications. Au contraire, ces enquêtes seraient limitées à l'intégration de métadonnées (voir *Glossaire*) et autres indicateurs qui indiqueraient une « probabilité » d'activité suspecte<sup>132</sup>. Si de tels renseignements peuvent être utilisés par les plateformes pour surveiller des acteurs à haut risque, comme l'indique la Virtual Global Taskforce, les métadonnées « sont généralement insuffisantes pour atteindre le niveau requis pour obtenir un mandat de perquisition »<sup>133</sup>. Au Royaume-Uni, la National Crime Agency (NCA) a attiré l'attention sur son enquête concernant David Wilson, un délinquant très actif en ligne, qui a utilisé de faux profils sur les réseaux sociaux pour leurrer au moins 500 jeunes garçons et se faire envoyer des images et vidéos sexuelles d'eux-mêmes ; il est ensuite passé au chantage et les a terrorisés. La NCA a averti que non seulement l'E2EE aurait réduit la probabilité de détection des infractions commises par Wilson, mais aurait pu également empêcher l'accès aux 250 000 messages qui ont permis de prouver la culpabilité du suspect et de le condamner<sup>133</sup>. Une utilisation accrue de l'E2EE pourrait également compromettre la détection des agressions dans les environnements non chiffrés, en réduisant l'accès aux matériels d'abus sexuels d'enfants nécessaire à l'apprentissage des systèmes de classification et autres outils de détection du contenu illégal.<sup>135</sup>

Des innovations sont en cours pour rendre les outils de détection compatibles avec l'E2EE. Le chiffrement « homomorphe » apparaît comme une solution potentielle car il offre un moyen d'analyser les données chiffrées sans les déchiffrer au préalable<sup>136</sup>. Les efforts de recherche sont axés sur l'amélioration de l'efficacité de la technologie afin de permettre un déploiement à grande échelle.

Parmi les autres propositions, citons:

- Intégrer des outils de détection dans les navigateurs et les systèmes d'exploitation des appareils (afin de réduire la dépendance à l'égard des plateformes pour la détection des abus).<sup>137</sup>
- Utiliser des « enclaves » sécurisées qui fourniraient un environnement protégé dans lequel déchiffrer, analyser et rechiffrer le contenu pour une transmission ultérieure.<sup>138</sup>
- Créer des signatures numériques pour le contenu au point de transmission. Celles-ci seraient transmises en même temps que le contenu chiffré, ce qui permettrait aux prestataires de services en ligne de filtrer les messages à partir des signatures (« hachages ») du matériels d'abus sexuels d'enfants connu.<sup>139 140</sup>

Aucune de ces solutions ne permettrait directement aux services de répression d'accéder au contenu: la police aurait quand même besoin des appareils des suspects ou des victimes pour prouver les infractions<sup>141</sup>. Toutefois, elles pourraient permettre une détection et un retrait plus proactifs du matériels d'abus sexuels d'enfants (par rapport à une démarche réactive déclenchée par des signalements d'utilisateurs ou des enquêtes policières)<sup>142</sup>. Les partisans de la protection de la vie privée pourront soutenir que ces mesures sont disproportionnées étant donné que, pour la majorité des internautes, les avantages du chiffrement de bout en bout sont plus importants que le problème de l'exploitation et des abus sexuels en ligne envers les enfants.<sup>143</sup>

#### **La coopération volontaire et la transparence doivent absolument compléter la réglementation pour consolider la riposte mondiale.**

En aidant les entreprises à équilibrer vie privée et sécurité des utilisateurs, la réglementation d'Internet pourrait atténuer partiellement l'impact du chiffrement de bout en bout sur la détection de l'exploitation et des abus sexuels en ligne envers les enfants. Les lois peuvent améliorer la prévention: le Canadian Centre for Child Protection considère que la réglementation est essentielle pour réduire les « niveaux élevés de récurrence de consultation des images » et les « longs délais de suppression » en offrant des incitations commerciales et juridiques « pour empêcher en premier lieu les images d'apparaître et de réapparaître ». <sup>144</sup>

La mise en œuvre de nouvelles lois pour régir Internet créera sans aucun doute des difficultés. Il s'agit d'un territoire inconnu pour de nombreux gouvernements et cela pose des questions difficiles, telles que:

- Comment empêcher les agressions sans restreindre indûment la liberté d'expression?
- Qu'entend-on par contenu « malveillant » (le contenu illégal est plus facile à définir)?
- Comment atténuer le risque que certaines lois aient un impact commercial disproportionné sur les entreprises de plus petite taille?

- Pour les entreprises disposant d'une base d'utilisateurs internationale, comment assurer la conformité avec la réglementation dans les différents pays?<sup>145</sup>

La consultation des prestataires de services en ligne et leur capacité d'adaptation seront essentielles au niveau de la mise en œuvre de la législation pour augmenter les chances que les lois apportent les avantages escomptés.

En fin de compte, une solution mondiale sera nécessaire: un accord international est la seule manière de réduire le risque de créer ce que l'e-Safety Commissioner australien qualifie de « "splinternet" juridique de l'Internet entre les textes des différents pays et régions ». De telles incohérences à l'échelle mondiale pourraient empêcher une surveillance efficace<sup>146</sup>, que ce soit du fait des sociétés ou des internautes eux-mêmes qui adapteraient leurs activités pour échapper à la réglementation. Il est possible qu'« à mesure que les grandes plateformes subissent la pression... il y ait un exode vers des espaces plus difficiles à contrôler et à modérer »<sup>147</sup>. Les bases d'utilisateurs de certaines des plus grandes plateformes semblent d'ores et déjà diminuer: le temps passé dans le monde sur les cinq applications de réseaux sociaux les plus téléchargées a chuté de 5% en 2020.<sup>148</sup>

Parallèlement, la coopération volontaire et la transparence sont indispensables pour compléter la réglementation. En plus de combler les écarts qui émergent entre les différents cadres réglementaires, elles permettent de réagir à une menace qui évolue rapidement.

La transparence de la part des prestataires de services en ligne est essentielle pour améliorer notre compréhension de la menace et ce qui permet de mettre en place une réponse efficace. À mesure que les outils de détection et d'élimination deviennent plus sophistiqués, la transparence est d'autant plus importante pour établir des normes cohérentes afin d'assurer une utilisation proportionnée de ces outils et d'« atténuer les craintes d'une "dérive" de la mission de la technologie et d'une utilisation abusive de celle-ci ».<sup>149</sup>

La coopération volontaire internationale a progressé (voir figure 11) parallèlement à l'innovation technologique. Des efforts sont encore à faire pour garantir que les initiatives soient inclusives au plan géographique et qu'elles impliquent l'éventail le plus large des acteurs jouant un rôle dans la prestation de services en ligne. Par exemple, en allant au-delà des plateformes vers les fabricants d'appareils et les opérateurs de réseaux mobiles.

Figure 11: Exemples de coopération internationale volontaire



**Le NCMEC a constaté une baisse de 58% des signalements sur CyberTipline au sein de l'UE lorsque l'utilisation de ce service a été interrompue par certaines entreprises en décembre 2020, afin de se conformer à la Directive européenne sur la protection de la vie privée.**

# Agressions

## Sollicitation d'enfants en ligne à des fins d'exploitation et d'abus sexuels

Comme de plus en plus d'enfants bénéficient d'un accès accru à Internet, le risque de voir s'intensifier les conséquences du grooming en ligne est important, à moins que des solutions de protection ne soient mises en œuvre.

En 2020, le NCMEC a relevé une augmentation de 97,5% de l'« incitation en ligne »<sup>153</sup>, une vaste catégorie d'exploitation qui englobe le grooming en ligne. Selon le NCMEC, cette catégorie inclut également « les adultes qui communiquent via Internet avec une personne supposée être un enfant dans l'intention de commettre un enlèvement ou une agression sexuelle »<sup>154</sup>.

L'enquête 2020 de NetClean menée auprès de 470 officiers de police dans 39 pays a également révélé une augmentation des tentatives de contact avec les enfants, confirmant l'hypothèse de l'augmentation de l'impact du grooming en ligne.<sup>155</sup>

Celui-ci peut souvent conduire à l'éventail complet de l'exploitation sexuelle des enfants: entre autres, la production d'images, la coercition, l'extorsion et les agressions physiques, dont les conséquences peuvent être graves. Une étude du NCMEC sur les signalements d'extorsion de faveurs sexuelles ou « sextorsion » enregistrés entre 2014 et 2016 a révélé que, parmi les victimes pour qui la résolution du crime n'a pas été positive, une sur trois s'était suicidée, avait tenté de le faire ou s'était automutiliée<sup>156</sup>. Il est prouvé que le grooming en ligne est également utilisé par les délinquants qui recrutent des enfants en vue d'une exploitation sexuelle basée sur une motivation commerciale.<sup>157</sup>

Il est difficile d'approfondir la prévalence du grooming en ligne car de nombreux pays ne l'ont pas encore défini dans la loi. Un benchmarking réalisé par Economist Impact en 2020 pour classer les ripostes des pays aux violences sexuelles sur enfants a révélé que, sur 60 pays étudiés, 21 seulement disposaient d'une législation interdisant les sollicitations en ligne à des fins sexuelles<sup>158</sup>. L'absence d'une définition juridique complique le signalement et les enquêtes aux niveaux national et international. Les sollicitations sont criminalisées dans la

« Convention de Lanzarote » (Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, voir le Glossaire).

Toutefois, cette définition suppose une proposition de rendez-vous suivie par des actes concrets conduisant à une rencontre. Elle nécessite donc une mise à jour pour répondre aux situations où l'abus est commis uniquement en ligne.<sup>159</sup>

**Les caractéristiques de l'environnement numérique ont créé de nouveaux facteurs de risque de sollicitations en ligne.**

Selon une étude de 2017, à l'âge de 12 ans, 50% des enfants dans le monde ont des comptes de réseaux sociaux<sup>160</sup>: une « empreinte » numérique qui « aide les prédateurs à s'immerger dans la vie des enfants avant d'établir un contact »<sup>161</sup>. Les informations recueillies grâce à des fonctions telles que la géolocalisation des images et l'« enregistrement » des lieux peuvent également être utilisées par les délinquants pour renforcer chez leurs victimes le sentiment d'être piégées ou pour localiser physiquement un enfant. Internet a également, d'une certaine manière, normalisé la communication avec des étrangers. L'enquête européenne KidsOnline 2020 a révélé que le contact en ligne avec une personne inconnue est une expérience courante pour 37% des enfants.<sup>162</sup>

Internet permet de mettre en œuvre des tactiques de grooming qui ne peuvent pas être reproduites dans le monde physique:

**« Pour les personnes ayant l'intention d'exploiter les enfants, il est beaucoup plus facile de jeter le filet le plus large possible aujourd'hui qu'il y a 20 ou 30 ans. Elles peuvent envoyer un millier de demandes en quelques jours et recevoir 999 refus. Il suffit d'une seule discussion ou demande d'ami(e) acceptée pour ouvrir la porte. »**

Thorn, avril 2021<sup>163</sup>

Une analyse des signalements de « coercition et extorsion de faveurs sexuelles auprès des enfants » enregistrés par le NCMEC entre

**2013 ————— 2016**

a révélé l'utilisation de multiples plateformes dans

**42%**

de cas.

Le nombre d'enfants qui réagissent à ces situations dépend de l'interaction de plusieurs facteurs. Depuis début 2020, ceux-ci comprennent notamment l'expérience individuelle de la COVID-19 chez les enfants. En tant qu'organisme caritatif britannique, le NSPCC avertissait: « Les sentiments de solitude suscités par la pandémie ont conduit certains enfants à chercher de la compagnie et du soutien auprès d'étrangers, les mettant ainsi plus à risque d'être sollicités »<sup>164</sup>.

**Les environnements en ligne offrent diverses opportunités à ceux qui cherchent à se livrer.**

L'utilisation de multiples canaux pour accéder à un plus grand nombre de victimes potentielles et éviter la détection est une tactique courante employée par les auteurs de grooming en ligne. Les délinquants cherchent systématiquement à transférer une conversation d'une plateforme publique vers un forum de messagerie privée — une technique désignée comme la communication « hors plateforme ». En général, les échanges sont déplacés vers des applications qui utilisent le chiffrement de bout en bout (ce qui garantit l'absence de surveillance des communications) ou des applications qui ne disposent pas d'outils intégrés pour détecter les comportements prédateurs. Les délinquants migrent fréquemment en grand nombre vers des plateformes plus récentes avec des mécanismes de sécurité et de modération sous-développés. Une analyse des signalements sur la « coercition en ligne et l'extorsion de faveurs sexuelles auprès d'enfants » consignés par le NCMEC entre 2013 et 2016 a révélé l'utilisation de multiples plateformes dans 42% des cas<sup>165</sup>. L'enquête d'Economist Impact, commanditée en même temps que ce rapport, a révélé que 68% des personnes interrogées ayant reçu du contenu sexuellement explicite en ligne pendant leur enfance l'avaient reçu par le biais d'un service de messagerie personnelle.

Les enfants rapportent avoir été approchés par les groomers « sur les réseaux sociaux, les applications de messagerie instantanée, les plateformes de streaming en direct et les services de chat vocal ou textuel intégrés aux jeux multijoueurs en ligne »<sup>166</sup>. Les plateformes de jeu posent des défis complexes pour la sécurité des enfants car, dans de tels environnements, les interactions entre adultes et enfants sont relativement normalisées. La socialisation dans le jeu est rendue possible par le chat audio et vidéo intégré et par des plateformes qui permettent aux joueurs de jouer en direct. Europol a mis en garde contre le fait que les enfants « sont plus exposés aux délinquants potentiels par le biais des jeux en ligne »<sup>167</sup>, en partie à cause de la COVID-19, et c'est ce qui expliquerait que la croissance du secteur des jeux en 2021 dépasse de 50% les prévisions précédentes<sup>168</sup>.

### MARIE COLLINS FOUNDATION: l'histoire d'Olivia

Olivia\* a fait l'objet de sollicitations sexuelles en ligne de la part de plusieurs délinquants pendant deux ans. Elle avait 10 ans lorsque l'agression a été découverte. Le principal agresseur l'avait approchée dans une application de jeu pour enfants avant de transférer les communications vers des applications plus privées.

Il avait partagé les coordonnées d'Olivia avec d'autres agresseurs, qui avaient commencé à la contacter directement, en lui envoyant des liens vers des vidéos pornographiques pour banaliser le comportement sexuel et lui « apprendre » ce qu'il fallait faire. Il s'agissait d'hommes de plusieurs pays différents, communiquant via le Dark Web.

Olivia avait fini par « divulguer » l'agression en laissant son appareil portable déverrouillé avec des e-mails des agresseurs à l'écran pour que son père les voie. Elle recevait des centaines d'e-mails d'hommes différents et n'était plus en mesure de garder le secret: elle avait peur et voulait que l'agression cesse.

Ces agressions ont eu un impact énorme sur sa santé mentale et son estime d'elle-même.

*La Marie Collins Foundation (MCF) est un organisme caritatif britannique dont l'objectif est de s'assurer que tous les enfants et les jeunes souffrant d'abus sexuels reçoivent un accompagnement pour se rétablir et aient ensuite des vies sûres et épanouissantes<sup>169</sup>.*

\* Pseudonyme

# La découverte des « mots masqués » révèle l'existence de contenus encore plus malveillants sur les plateformes de jeux.



La nature anonyme et sans frontières d'Internet, ainsi que la facilité d'accès à des espaces perçus comme sûrs en ligne, mettent les agresseurs en confiance pour partager le matériels d'abus sexuels d'enfants, ainsi que les tactiques et les « techniques de dissimulation » permettant d'échapper à la détection via les réseaux de délinquants.

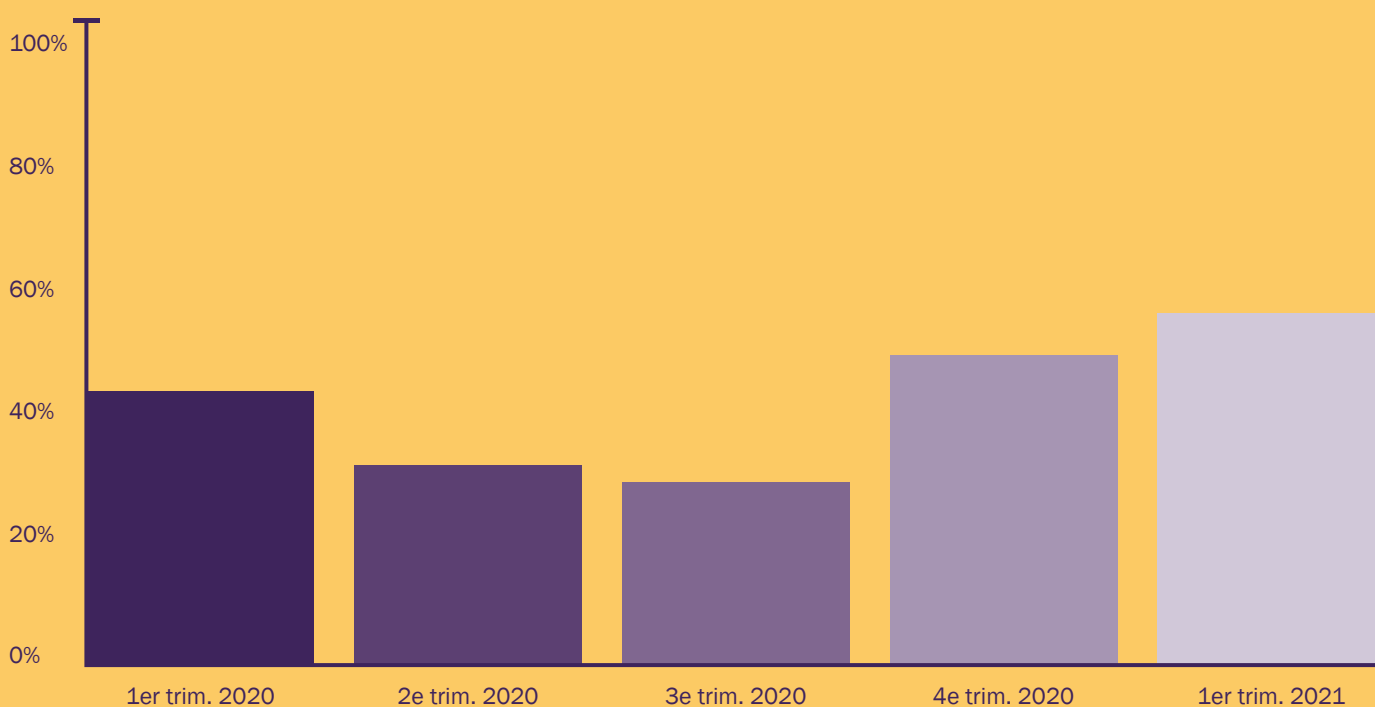
Dans le secteur des jeux, les salles de chat, les appels vocaux et la diffusion en direct ont offert de nouveaux moyens aux délinquants d'établir des contacts avec les enfants et d'entamer un processus de grooming. Une analyse de Crisp sur les conversations du Dark Web faisant allusion à trois plateformes de jeu mondiales très populaires a révélé un dialogue continu entre les délinquants, manifestement pour partager des conseils utiles à propos des sollicitations. Le nombre de conversations a augmenté en moyenne de 13% sur l'ensemble des plateformes entre 2019 et 2020.

Crisp a également observé l'utilisation permanente de « mots masqués » par les délinquants sur les plateformes elles-mêmes. Il s'agit de mots dans lesquels des lettres-clés sont remplacées par des chiffres ou des symboles afin d'éviter les méthodes de détection (par exemple, taper « 8!rthday » au lieu de « Birthday »). En identifiant le moment où les délinquants tentent de masquer des mots sur les plateformes, Crisp a mis au grand jour 50% de contenu supplémentaire dans lequel ces mots étaient utilisés, ce qui a permis d'identifier un volume plus important de contenus malveillants, ainsi que leurs auteurs malintentionnés.

Dans les jeux ou sur n'importe quel réseau social/plateforme de contenus produits par l'utilisateur, la sécurité des utilisateurs exige la capacité d'identifier rapidement le contenu malveillant et les stratégies associées. L'utilisation de ces informations est essentielle pour identifier les délinquants et mettre à jour les politiques afin de prévenir les agressions futures.

Figure 12: Contenu supplémentaire découvert avec l'identification des mots masqués

## Pourcentage de contenu supplémentaire comportant des mots-clés lors de la recherche de mots masqués



**Il existe des solutions pour détecter les sollicitations en ligne, mais leur adoption est peu répandue et les défis techniques persistent.**

On utilise déjà certains outils s'appuyant sur l'intelligence artificielle pour identifier et bloquer les conversations sur le grooming des enfants. Cependant, seulement 37% des entreprises ayant répondu à une enquête WeProtect Global Alliance/Technology Coalition ont déployé cette technologie<sup>170</sup>.

La détection du grooming en ligne présente des difficultés. Le développement des outils repose sur l'accès des développeurs aux scripts de chat de grooming pour créer des algorithmes. Bien qu'il y ait des exemples de collaboration efficace entre la police, les plateformes et les développeurs, il existe une marge d'amélioration dans le partage des données pour renforcer l'innovation. Parmi les autres difficultés, citons le développement d'outils pouvant fonctionner dans plusieurs langues et surmonter l'utilisation d'argot et de noms de code. Une innovation permanente est indispensable pour améliorer la précision de ces outils et permettre ainsi de minimiser également les intrusions injustifiées dans la vie privée des utilisateurs.

Les solutions les plus efficaces sont celles capables de détecter les conversations à haut risque pour empêcher les sollicitations de se produire. De telles technologies sont toutefois complexes, notamment parce qu'« une conversation peut évoluer très rapidement... elle peut prendre un aspect sexuel en moins de trois minutes »<sup>171</sup>. La plupart des outils de détection des sollicitations ne sont pas facilement déployables dans les environnements E2EE.

**La fréquence du grooming en ligne pourrait être considérablement réduite si l'on rendait les environnements en ligne sûrs dès leur conception (« Safe by Design »).**

« Safety by Design » est une initiative de l'e-Safety Commissioner australien, aujourd'hui reconnue dans le monde entier, qui fait de la sécurité de l'utilisateur un « principe fondamental de conception à intégrer dès le départ dans le développement des innovations technologiques »<sup>172</sup>.

Les solutions « Safety by Design » ayant le plus grand potentiel de réduire le risque de sollicitations en ligne sont notamment les outils d'estimation et de vérification de l'âge. Ces technologies sont encore relativement embryonnaires<sup>173</sup>, mais pourraient être utilisées pour exclure les prédateurs des forums d'enfants et garantir des expériences en ligne adaptées à l'âge. Parmi d'autres exemples, nous pouvons citer le contrôle parental et les filtres de contenus. De nombreuses grandes plateformes intègrent déjà certaines de ces solutions:

- La plateforme de jeux **Roblox** dispose d'un logiciel de sécurité intégré bloquant le contenu explicite et empêchant les jeunes utilisateurs de partager leurs coordonnées<sup>174</sup>.
- La plateforme de réseau social **TikTok** a introduit des paramètres de confidentialité et de sécurité par défaut pour les moins de 18 ans<sup>175</sup>.
- **Instagram** ajoute des fonctions de sécurité pour protéger les adolescents contre les messages indésirables directs d'adultes qu'ils ne connaissent pas<sup>176</sup>.
- **YouTube** a créé des « expériences supervisées » pour les enfants de moins de 13 ans, limitant leur capacité à télécharger du contenu, à discuter ou à recevoir des commentaires, et aidant les parents à gérer le contenu auquel les enfants ont accès<sup>177</sup>.

En informant les enfants sur les risques en ligne et en réduisant les possibilités offertes aux délinquants, ces fonctions peuvent réduire le risque que les enfants deviennent victimes de sollicitations en ligne. Elles peuvent également accroître l'efficacité d'autres mécanismes de sécurité par la diminution du volume global d'incidents, permettant ainsi une surveillance et une protection plus ciblées.

## **YOTI: TECHNOLOGIE D'ESTIMATION DE L'ÂGE**

YOTI est une plateforme d'identification mondiale basée au Royaume-Uni, dotée d'une technologie d'estimation de l'âge.

Le système d'intelligence artificielle de YOTI analyse le visage d'une personne et estime son âge en 1 à 1,5 seconde sans révéler ni conserver aucune donnée personnelle. Son taux de précision moyen est actuellement de 2,19 ans, tous âges confondus, et de 1,5 an pour les 13-25 ans, ce qui garantit une modération adaptée à l'âge avec les seuils d'âge standard du secteur. YOTI intègre également les 13% de la population mondiale qui ne possèdent pas de photo d'identité.

À ce jour, la technologie d'estimation de l'âge de YOTI a effectué plus de 500 millions de contrôles de l'âge pour des organisations partenaires, notamment dans la diffusion en direct, le commerce électronique, chez les adultes, dans les jeux et chez les opérateurs de télécommunications.

**Nous devons améliorer notre compréhension du grooming en ligne pour permettre une détection et une prévention efficaces et permanentes.**

L'efficacité des interventions risque d'être réduite si nous ne comblons pas nos lacunes en matière de connaissances et de recherches.

Nous ne comprenons toujours pas bien l'interaction entre les sollicitations « physiques » et en ligne, ni les complexités des interventions pour empêcher de tels abus, en particulier si l'agresseur est connu de l'enfant (comme dans la plupart des cas des sollicitations « physiques »)<sup>178</sup>. Dans ce contexte, il est nécessaire d'améliorer notre compréhension des parcours vers la délinquance des agresseurs qui sollicitent les enfants en ligne, ainsi que des facteurs de risque et de protection qui influent sur la probabilité qu'un enfant soit agressé. Il a été observé, par exemple, que les enfants handicapés peuvent présenter des vulnérabilités particulières parce qu'ils se tournent vers Internet pour compenser un manque de soutien ou de relations dans le monde réel<sup>179</sup>. Les idées sur ces questions peuvent être utilisées pour concevoir des interventions adaptées et fortes afin de protéger les enfants et réduire encore, voire supprimer les opportunités pour les délinquants.

# 06 Agressions

## Production de matériels d'abus sexuels d'enfants

Lorsqu'une agression sur un enfant est documentée, son auteur est aussi coupable de production de matériels d'abus sexuels d'enfants.

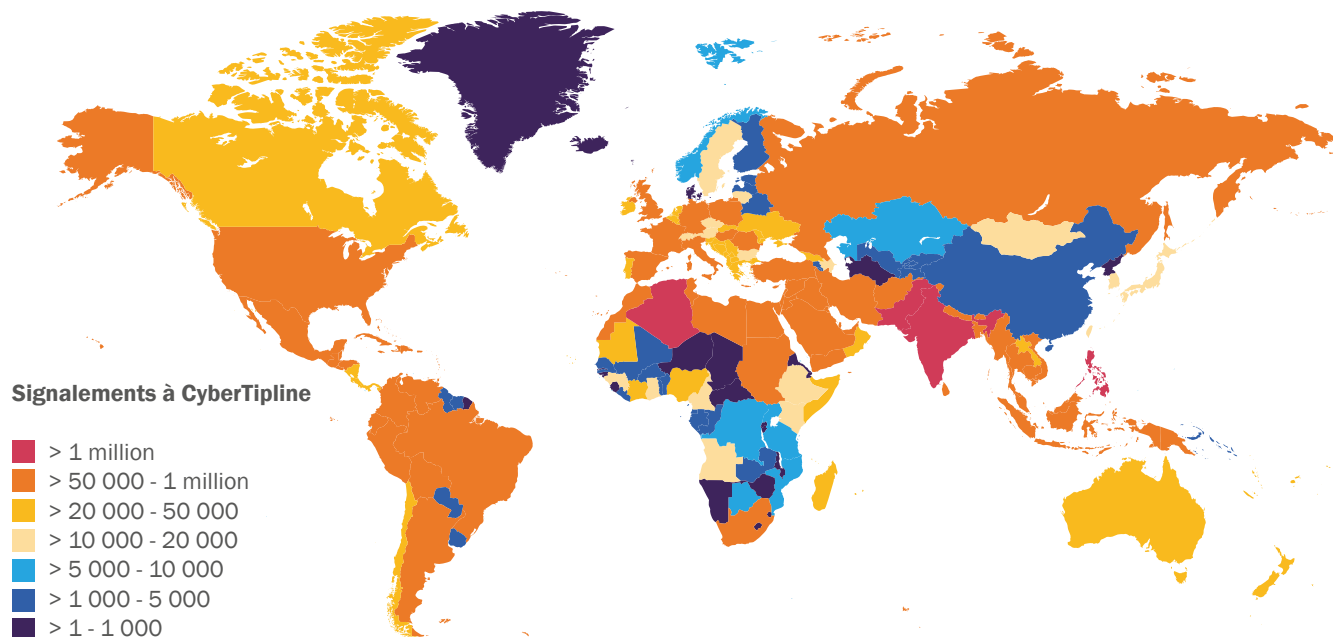
Les délinquants évoluent dans leurs méthodes de production, généralement pour profiter des nouvelles technologies.

La production de matériels d'abus sexuels d'enfants existe vraisemblablement dans toutes les régions du monde. Des filles de tous les âges apparaissent le plus souvent dans les images.


Une étude conjointe réalisée par Thorn, Google et NCMEC en 2019 a révélé que 81% des cas de violence sexuelle envers des enfants étaient commis en Asie, Afrique et Europe<sup>180</sup>. Les dernières données du NCMEC (voir figure 13 ci-dessous) indiquent que ces mêmes régions, plus les Amériques, continuent à produire une grande partie des signalements.

Malheureusement, ces données offrent une vision naturellement limitée des tendances mondiales. D'un côté, l'origine des signalements peut être différente de l'origine des images. De plus, les signalements ne donnent que la mesure du problème « connu ». Il est fort probable que la production soit plus importante dans les pays où il y a moins ou pas de mécanismes en place pour la détecter. Ceci semble confirmé par les résultats de l'enquête d'Economist Impact, selon laquelle les enfants subissent des agressions sexuelles en ligne dans toutes les régions du monde.

Figure 13: Origines des signalements de soupçon d'exploitation sexuelle d'enfants reçus par le service CyberTipline du NCMEC en 2020. Publié avec la permission du NCMEC<sup>181</sup>.







En allant plus loin dans les biais géographiques concernés, preuve est faite que les enfants d'Amérique du Nord et d'Europe occidentale sont plus susceptibles d'être identifiés dans des images d'agression que ceux d'Europe de l'Est et d'Asie du Sud-est, probablement en raison de protocoles plus avancés dans le signalement et l'identification des victimes<sup>182</sup>. Ce schéma est symptomatique des inégalités mondiales qui changent l'impact local des abus et modifient la forme de la menace dans son ensemble.

En 2020, INHOPE a évalué 267 192 URL de contenu illégal, dont 93% concernaient de jeunes victimes féminines<sup>183</sup>. L'IWF, un partenaire proche d'INHOPE, rapporte la même proportion de contenu présentant des filles dans les URL évaluées par son équipe<sup>184</sup>. Mais cela ne signifie pas nécessairement que les filles sont plus victimes d'agressions que les garçons. En réalité, l'enquête d'Economist Impact n'a révélé qu'une légère différence dans les expériences d'agressions sexuelles en ligne signalées par les participants masculins et féminins. Les agressions sur les garçons sont peut-être simplement moins documentées. Cela peut néanmoins suggérer que les filles sont plus susceptibles de connaître des agressions prolongées du fait de la production, du partage et de la diffusion ultérieure de leur image.

**Le matériels d'abus sexuels d'enfants est souvent produit par des membres de la famille. Cela crée une série de défis pour la détection et la prévention.**

Selon l'IWF, le contenu à caractère sexuel « autoproduit » par les enfants présente essentiellement des enfants à domicile<sup>185</sup>. Au cours de l'année écoulée, un surcroît de production dans les environnements domestiques a également été attribué aux groupes de délinquants qui adaptent leurs modes de travail à la COVID-19, « faisant grimper l'utilisation des communications en ligne et l'exploitation à domicile »<sup>186</sup>. Cependant, si la plupart des images sont produites dans les foyers familiaux, c'est aussi parce que le matériels d'abus sexuels d'enfants est fréquemment produit par des membres de la famille:

- Une étude sur les cas de violence sexuelle chez les enfants en Colombie a révélé que les délinquants se trouvaient généralement dans le cercle de confiance de l'enfant, voire dans son noyau familial<sup>187</sup>.
- Au Mexique, 73% des délits de violence sexuelle contre les enfants sont commis par les parents et 75% des agressions se produisent dans le foyer des victimes<sup>188</sup>.
- Une étude menée auprès de 150 adultes ayant survécu à des agressions sexuelles en Australie a révélé que 42% d'entre eux avaient identifié leur père biologique, adoptif ou beau-père comme étant leur principal agresseur et producteur du matériels d'abus sexuels d'enfants<sup>189</sup>.

### Ministère américain de la Justice : « BabyHeart », un site du Dark Web

« BabyHeart » était un site du Dark Web dédié aux abus sur enfants de cinq ans et moins. Il a été accessible au public pendant plus de deux ans et, au cours de cette période, le nombre de ses membres a atteint des centaines de milliers. Les délinquants utilisateurs du site ont expliqué leur préférence pour les enfants de cette tranche d'âge parce qu'ils étaient perçus comme moins susceptibles ou incapables de déclarer l'abus et qu'ils étaient donc considérés comme présentant moins de risques. La plupart des images partagées sur BabyHeart ont sans aucun doute été produites dans le cadre d'agressions familiales ou d'autres contextes de garde d'enfants. Cela souligne clairement l'importance de recourir à des mécanismes de prévention et de détection qui ne reposent pas sur la dénonciation par les enfants et ne supposent pas que les familles protègent les enfants<sup>194</sup>.

- Une étude sur les cas d'agressions d'enfants en Espagne a révélé que, dans 80,2% des cas, le délinquant appartenait au cercle de confiance de la victime et que, dans 32% des cas, il s'agissait de leur père biologique<sup>190</sup>.

Avoir subi une agression sexuelle des mains d'un membre de sa famille peut créer un traumatisme supplémentaire et complexe, en particulier parce que ce type d'abus commence souvent lorsque les victimes sont plus jeunes et dure plus longtemps<sup>191</sup>. Les victimes d'agressions familiales sont également les moins susceptibles de les divulguer, et l'auto-signallement est généralement faible chez les enfants victimes d'abus sexuels. Seulement 2% des signalements sur le service CyberTipline du NCMEC proviennent des enfants eux-mêmes<sup>192</sup>.

Malgré les progrès importants réalisés dans les technologies d'analyse d'images et de reconnaissance faciale, les taux d'identification des victimes demeurent faibles dans l'ensemble. En avril 2021, le Canadian Centre for Child Protection avait traité 126 milliards d'images dans le cadre de son projet Arachnid, dont 85% présentaient des victimes toujours non identifiées<sup>193</sup>. Les difficultés liées à l'identification des victimes soulignent l'importance cruciale d'informer toutes les communautés et d'investir dans les systèmes de protection de l'enfance pour améliorer la détection des abus, afin que les victimes puissent être identifiées et protégées.

L'Australian Centre to Counter Child Exploitation a identifié le « capping » comme la tendance délinquante actuelle posant le plus de problèmes et générant environ

**60%–70%**

des signalements à l'Unité d'identification des victimes.

En 2020, un « bot » d'intelligence artificielle opérant sur Telegram a généré

**100,000**

des « deepfakes » pornographiques de vraies femmes et jeunes filles.

**Les délinquants font évoluer leurs modes de production. Certains sont dissimulés et les enfants ne sont peut-être même pas conscients d'être des victimes.**

Le « capping » est devenu plus répandu ces dernières années, et des services de police ont signalé une augmentation significative de ce type de délinquance pendant la pandémie de COVID-19<sup>195</sup><sup>196</sup><sup>197</sup>. Il suppose généralement des sollicitations et une coercition sexuelle sur les enfants et a été associé à l'augmentation du contenu « autoproduit » par les enfants. Les délinquants ciblent les enfants sur différentes plateformes et cherchent à gagner leur confiance, avant de les contraindre à effectuer des actes sexuels filmés. Le contenu est ensuite partagé dans des forums du Dark Web. Selon Europol, le nombre de fils de discussion et de messages dans une section destinée aux « cappers » dans un forum du Dark Web a plus que triplé entre décembre 2019 et février 2020<sup>198</sup>.

L'Australian Centre to Counter Child Exploitation a identifié le « capping », qui est à l'origine d'environ 60 à 70% des signalements à son unité d'identification des victimes, comme la tendance actuelle la plus problématique. Le « capping » illustre également le potentiel de « ludification » (voir *glossaire*) des agressions. Un site sur le Dark Web, surveillé par les forces de l'ordre, organise des concours mensuels et des « batailles de capping », où les cappers s'affrontent en publiant des images d'agressions<sup>199</sup>.

Si certains enfants savent qu'ils ont été victimes de « capping », d'autres n'en sont peut-être pas conscients. La création secrète de matériels d'abus sexuels d'enfants est une tendance de production élargie, facilitée par une gamme d'appareils numériques, notamment les webcams (parfois piratées) et les caméras de sécurité à domicile ou dans les établissements scolaires. En Corée du Sud, ce phénomène, connu sous le nom de « molka », est intensifié par le déploiement de caméras d'espionnage dans les objets du quotidien comme les stylos<sup>200</sup>.

**Des technologies telles que l'imagerie générée par ordinateur (CGI) peuvent permettre une diversification de la production et exiger d'apporter des modifications à la législation.**

Actuellement, les « deepfakes » (hypertrucages) et la « CGI » ne sont pas fréquents dans les enquêtes sur les agressions infligées aux enfants<sup>201</sup>. Cependant, ils risquent de devenir plus courants. En 2020, un « bot » d'intelligence artificielle opérant sur Telegram a généré 100 000 « deepfakes » pornographiques de vraies femmes et jeunes filles<sup>202</sup>. Dans le même ordre d'idées, le secteur du cybersexe en réalité virtuelle pour adultes a connu une croissance significative, en partie attribuée à l'impact des confinements dus au COVID-19<sup>203</sup>. L'e-Safety Commissioner australien a exprimé son inquiétude quant à l'utilisation potentielle de la réalité virtuelle et d'autres technologies immersives en tant qu'« outil d'abus sexuel en ligne sur les enfants »<sup>204</sup>.

## Imagerie générée par ordinateur (CGI) et « deepfakes »

La CGI est la création de contenus visuels fixes ou animés avec un logiciel d'imagerie<sup>205</sup>. Dans le contexte des abus sexuels envers les enfants, il s'agit d'images sexualisées d'enfants, créées entièrement ou partiellement de façon artificielle ou numérique<sup>206</sup>. Le « deepfake » est une forme de CGI qui utilise l'intelligence artificielle (IA) pour remplacer l'image d'une personne par une autre dans des photos ou des vidéos enregistrées<sup>207</sup>.

Les principales préoccupations sont le manque d'obstacles à l'utilisation des résultats et à leur nature convaincante. Même les simples filtres intégrés aux applications les plus courantes sont capables de transformer du contenu en un clic. Certains types d'images de synthèse pourraient créer des défis en matière de priorité pour les services de police s'il devient difficile de distinguer un véritable enfant d'un personnage artificiel<sup>208</sup>.

Cependant, les techniques de CGI et les technologies associées sont peu susceptibles de dominer dans cet espace en l'état actuel des choses, principalement en raison de la disponibilité en ligne de matériels d'abus sexuels d'enfants photographique. Toutefois, elles méritent d'être prises en considération, notamment parce qu'elles réaffirment la nécessité d'une position concertée à l'échelle internationale sur une gamme de matériel non photographique qui contribue à la croissance de la menace : par exemple, la CGI, les « deepfakes », les animations, les caricatures et les dessins illustrant des abus sexuels sur des enfants, ainsi que les « poupées à usage sexuel » de type enfant vendues sur Internet.

La CGI est néfaste car « elle est connue pour être utilisée dans le grooming d'enfants... elle alimente des fantasmes très réels, encourage la propension des délinquants à commettre des abus et contribue à maintenir un marché pour le matériel destiné aux agressions sexuelles sur les enfants »<sup>209</sup>. Il existe de nombreuses preuves à l'appui de cette position, notamment la présence fréquente de ce type de matériel aux côtés de photographies d'enfants à caractère sexuel<sup>210</sup>. Pourtant, très peu de pays ont inscrit un principe de cet ordre dans leur législation<sup>211</sup>.

La CGI peut également être utilisée pour mettre en place de puissantes techniques de démantèlement, comme en témoigne le cas de « Sweetie », une image d'enfant créée par CGI qui a servi à piéger plus de 1 000 prédateurs<sup>212</sup>. De nombreux réseaux de délinquants exigent de leurs membres potentiels qu'ils partagent du nouveau matériel pour entrer dans des groupes fermés ; des images artificielles pourraient également être utilisées pour aider la police à infiltrer de telles communautés. La collaboration mondiale des forces de l'ordre est essentielle pour désamorcer l'utilisation plus large de ces tactiques ; un consensus est également nécessaire sur l'éthique d'un déploiement technologique à de telles fins<sup>213</sup>.

# Agressions

## Recherche et/ou consultation de matériels d'abus sexuels d'enfants

Les tentatives d'accès à du matériels d'abus sexuels d'enfants sont en augmentation. Pour une prévention durable à long terme, il est essentiel de s'attaquer à la fois aux aspects « offre » et « demande » de la question.

La plupart du matériels d'abus sexuels d'enfants est accessible via le Web de surface, les applications de chiffrement de bout en bout ou le partage pair-à-pair (P2P).

Trois clics seulement peuvent suffire pour découvrir du matériels d'abus sexuels d'enfants sur Internet<sup>214</sup>. La plupart de celui-ci est accessible de cette façon: via le Web de surface ou les réseaux P2P<sup>215</sup>. Selon Interpol, l'utilisation de ces derniers a progressé au cours de 2020<sup>216</sup>.

On constate que beaucoup de personnes condamnées pour consultation de matériels d'abus sexuels d'enfants n'ont fait aucune ou que peu de tentative pour couvrir leurs pistes<sup>217</sup>, bien que cet échantillon soit bien évidemment quelque peu faussé. Comme il est souligné dans la section *Technologie* du chapitre « Thème », une partie des délinquants utilisent des outils et des méthodes de pointe pour échapper à la détection. Une des techniques documentées est celle qui consiste à créer des applications dirigeant les utilisateurs vers des groupes de messagerie fermés servant au partage d'images<sup>218</sup>. Selon Europol, la distribution d'images d'abus sexuels d'enfants « a lieu régulièrement sur les plateformes de réseaux sociaux »<sup>219</sup>.

Les délinquants utilisent souvent des plateformes et des applications E2EE, c'est-à-dire des environnements qui combinent l'accessibilité du Web de surface à un niveau élevé de sécurité. Comme l'indique le rapport 2021 d'Europol sur l'évaluation de la menace que représente la grande criminalité organisée, « l'utilisation généralisée d'outils de chiffrement, y compris les applications de chiffrement de bout en bout, a réduit le risque de détection » pour ceux qui agressent les enfants<sup>220</sup>. L'utilisation d'applications crée des défis importants pour les forces de l'ordre, car elles doivent infiltrer des groupes de messagerie fermés pour obtenir des preuves des infractions.

Une fois l'entrée obtenue, de nombreux services de police se limitent à la collecte manuelle de données. La Child Rescue Coalition pilote le développement d'une solution pour rationaliser l'acquisition de preuves en temps réel à partir d'applications d'appareils mobiles. L'outil est conçu pour être utilisé par des officiers de police ayant infiltré des groupes de délinquants. En réduisant le besoin de collecte manuelle de données, il pourrait améliorer considérablement l'efficacité des opérations d'infiltration. La collaboration continue avec les forces de l'ordre internationales est essentielle pour maximiser leur impact et s'assurer qu'elles soutiennent l'amélioration de l'identification et de la protection des victimes<sup>221</sup>.

**Le Dark Web cache le contenu le plus déviant et permet le partage et la mise en réseau entre les communautés de délinquants.**

### Dark Web

Il s'agit de la couche d'informations et de pages accessibles uniquement par le biais de réseaux superposés (tels que les réseaux VPN (Virtual Private Networks) et P2P (Peer-to-Peer)) qui réduit l'accès public. Les utilisateurs ont besoin d'un logiciel spécial pour accéder au Dark Web car celui-ci est essentiellement crypté et la plupart des pages du Dark Web sont hébergées de manière anonyme<sup>222</sup>.

Globalement, l'activité de ce réseau a augmenté de 300% au cours des trois dernières années<sup>223</sup>. Le Dark Web serait un centre de contenus plus jeunes<sup>224</sup> et plus déviants<sup>225</sup> sur l'exploitation et les abus sexuels en ligne envers les enfants.

Les communautés de délinquants sur ce réseau persistent et évoluent depuis plus de dix ans. En ce sens, elles ne représentent pas une nouvelle dimension de la menace. Mais ce qui a changé, c'est la disponibilité de solutions d'anonymat, comme Tor et les VPN, qui sont maintenant courantes et même intégrées par défaut dans certains navigateurs Web<sup>226</sup>.

## Tor

« Tor » est un réseau en open source qui garantit la confidentialité et permet aux utilisateurs de naviguer sur le Web de façon anonyme. Ce système utilise une série de nœuds superposés pour masquer les adresses Web, les données en ligne et l'historique de navigation<sup>227</sup>.

Aujourd'hui, les individus ont besoin d'un minimum de connaissances techniques pour masquer leur activité en ligne. Pour les forces de l'ordre, le défi consiste à garder une longueur d'avance sur les délinquants qui sont davantage en mesure d'utiliser ces capacités, qui leur accordent un anonymat immédiat pour leur permettre d'éviter de se faire prendre<sup>228 229 230</sup>.

**. Les tentatives d'accès à du matériels d'abus sexuels d'enfants augmentent. Les données semblent indiquer l'existence d'un lien entre l'exposition habituelle à un contenu sexuel adulte déviant et la consultation de matériels d'abus sexuels d'enfants.**

En 2020, 8,8 millions de tentatives de récupération de matériels d'abus sexuels d'enfants ont été suivies par trois organisations membres de l'IWF en seulement un mois<sup>231</sup>. Au cours des confinements dus à la pandémie de COVID-19 en Inde, il y a eu une augmentation de 95% des recherches de matériels d'abus sexuels d'enfants<sup>232</sup>. Le Conseil des droits de l'homme de l'ONU a également signalé une hausse de 25% de la demande de matériels d'abus sexuels d'enfants durant la pandémie dans certains États membres de l'Union européenne<sup>233</sup>.

On estime avec prudence que 1% de la population mondiale de sexe masculin est touchée par la pédophilie (attirance sexuelle pour les enfants prépubères)<sup>234</sup>. Nombre de ces individus cherchent à voir sciemment du matériels d'abus sexuels d'enfants pour répondre à leurs désirs sexuels<sup>235</sup>.

Des capacités de répression avancées sont essentielles pour identifier ce type de délinquants et gérer les risques associés – y compris leur éventuelle progression vers la perpétration d'abus physiques contre des enfants.

Il y a beaucoup d'autres moyens de consulter du matériels d'abus sexuels d'enfants. Selon la Fondation Lucy Faithfull, seuls 15 à 20% des délinquants avec lesquels elle travaille actuellement sont des pédophiles « dans la mesure où les enfants prépubères représentent leur principal intérêt sur le plan sexuel »<sup>236</sup>. Plusieurs études ont établi un lien entre la consultation de matériels d'abus sexuels d'enfants et l'exposition habituelle à la pornographie adulte déviante: supposément parce que ce comportement peut provoquer une désensibilisation et créer le désir de rechercher des stimuli plus graves pour continuer à atteindre le même niveau d'excitation sexuelle<sup>237 238</sup>. Les deux domaines qui posent particulièrement problème sont la « pornographie sur le thème des agressions » et la pornographie qui cherche à représenter des adultes comme des enfants. La première permet aux spectateurs de « passer à l'étape suivante, à savoir la consultation d'abus réels » ; la seconde est décrite par les délinquants comme une passerelle vers la consultation de matériels d'abus sexuels d'enfants<sup>240</sup>.

Le lien avec la consultation d'images pornographiques déviantes est inquiétant, étant donné que l'exposition des enfants au contenu sexuel adulte a considérablement augmenté à l'ère numérique. Des études menées dans plusieurs pays d'Asie de l'Est suggèrent que 50% des enfants et des jeunes ont été exposés à des « médias sexuellement explicites », tandis que les États-Unis, l'Australie et un certain nombre de pays européens signalent des taux d'exposition de 80% ou plus<sup>241</sup>. L'observation fréquente d'activités pornographiques adultes ou de pornographie violente depuis le plus jeune âge est associée à la consultation de matériels d'abus sexuels d'enfants<sup>242</sup>.

La façon dont les utilisateurs sont invités à interagir avec le contenu en ligne contribue également à accélérer les parcours vers la délinquance. La recommandation de contenu constitue le principal moyen de stimuler l'engagement des utilisateurs sur les plateformes de réseaux sociaux. En général, il existe deux modèles pour cela. Le premier est le modèle algorithmique de « graphe social », qui présuppose les intérêts des utilisateurs en donnant la priorité à leurs activités sur le plan des relations. Le second est le modèle de « graphe d'intérêt », qui déduit les intérêts des utilisateurs en fonction de leurs activités et de leurs engagements passés. Ces algorithmes risquent d'encourager le comportement des utilisateurs qui cherchent de manière inappropriée du contenu impliquant des enfants, en leur recommandant de façon réitérée des images et vidéos similaires<sup>243 244</sup>. Ceci conjugué au nombre élevé de vidéos vues et de fils les accompagnant avec des commentaires troublants, qui échappent souvent à l'attention des modérateurs<sup>245</sup>, a pour résultat d'effacer les inhibitions internes et de favoriser les abus<sup>246 247</sup>. Certaines grandes plateformes affirment avoir des mécanismes de détection et des politiques de modération en place pour soutenir l'identification de tels comportements<sup>248</sup>. La rapidité et l'efficacité de ces mesures sont essentielles car, comme l'explique le National Centre for Social Research au Royaume-Uni, « la désensibilisation/désinhibition en ligne et la validation de la part d'autres délinquants sont souvent de bonnes raisons de regarder du matériels d'abus sexuels d'enfants et/ou de passer à une agression physique »<sup>249</sup>.

**. La suppression des recherches de matériels d'abus sexuels d'enfants peut dissuader la délinquance. Mais l'impact de telles interventions est difficile à mesurer.**

Le lien mis en évidence entre le contenu affiché et les abus physiques montre pourquoi l'interruption des tentatives de recherche d'images est si importante.

La majorité (60%) des entreprises interrogées dans le cadre d'une enquête WeProtect Global Alliance/Technology Coalition Tech ont confirmé qu'elles émettaient une forme de messages de dissuasion<sup>250</sup>. Le filtrage des recherches est un mécanisme répandu, utilisé principalement par les moteurs de recherche. Les demandes des utilisateurs sont recoupées avec une liste de contenus à bloquer, de sorte que si une correspondance est trouvée, aucun résultat n'est renvoyé. Dans certains cas, un avertissement est également adressé à l'auteur de la requête. Quand ce filtrage a été mis en œuvre par Google et Microsoft, en l'espace d'un an, le nombre total de recherches d'images d'agressions sur le Web a diminué de 67%<sup>251</sup>.

Dans une étude financée par le gouvernement australien, il a été observé que les messages d'avertissement en ligne adressés aux utilisateurs cherchant à consulter de la « pornographie à l'extrême limite de la légalité » ont augmenté de 25% les taux d'attrition<sup>252</sup>. De la même manière, la campagne « Stop IT Now! » de la Fondation Lucy Faithfull au Royaume-Uni et le projet de prévention Dunkelfeld en Allemagne ont tous deux démontré que la dissuasion peut promouvoir la recherche d'aide chez les délinquants (potentiels)<sup>253</sup>. L'Oak Foundation s'est récemment engagée à financer un nouveau projet de recherche visant à identifier et évaluer les initiatives de prévention de la délinquance et à renforcer la capacité de les mettre en œuvre par le biais d'un hub en ligne pour les responsables politiques et praticiens<sup>254</sup>.

## LUCY FAITHFULL FOUNDATION: COLLABORATION AVEC MINDGEEK (PORNHUB)

La Lucy Faithfull Foundation (la Fondation) est une association caritative britannique qui contribue à la prévention des violences sexuelles infligées aux enfants, notamment en travaillant avec des adultes et des jeunes ayant commis des abus sexuels ou risquant d'en commettre. En février 2021, la Fondation a lancé une collaboration avec Mindgeek pour qu'il diffuse des messages de dissuasion sur son site Web de pornographie pour adultes, Pornhub. Ces messages s'affichent lorsque les utilisateurs effectuent des recherches indiquant qu'ils essaient de trouver des vidéos sexuelles mettant en scène des enfants. Mindgeek avait déjà reconnu la nécessité d'afficher des messages dissuasifs sur ses sites de contenu pour adultes, où il avait remarqué des tentatives par une petite minorité d'utilisateurs de rechercher du matériels d'abus sexuels d'enfants en utilisant des termes de recherche interdits.

Ces messages de dissuasion précisent la loi applicable et le préjudice causé aux enfants par la création et la consultation de ce matériel. Ils orientent également les utilisateurs vers une assistance pour les inciter à interrompre tout comportement illégal, notamment vers « Stop It Now! Get Help », un service autonome d'intervention sur Internet à destination des personnes préoccupées par leur comportement sexuel en ligne envers les enfants. De février à début mai 2021, ces messages de dissuasion ont conduit plus de 35 000 utilisateurs à travers le monde à contacter « Stop IT Now! Get Help ». Bien qu'il s'agisse d'un tout petit nombre par rapport aux volumes de trafic globaux sur Pornhub, comme l'a souligné la Fondation Lucy Faithfull, ces messages jouent un rôle important dans l'éducation et l'intervention.

La principale difficulté de la dissuasion est la mesure de l'efficacité. Dans les exemples cités dans ce document, cette mesure a été obtenue en surveillant la consultation des documents d'aide et les comportements de recherche d'assistance. Mais tout ceci est limité, notamment parce qu'il est impossible de savoir si les infractions ont été effectivement dissuadées et comment elles l'ont été. Il y a également des questions sur l'impact de la dissuasion à long terme: les utilisateurs ne risquent-ils pas devenir insensibles aux avertissements au fil du temps ou simplement de se déplacer vers d'autres sites?

**Les mécanismes de dissuasion sont un élément essentiel d'une riposte plus large prenant en compte l'ensemble des voies amenant les gens à consulter du matériels d'abus sexuels d'enfants.**

L'importance des efforts réalisés pour supprimer ce matériel d'Internet est incontestable. Toutefois, faute de travailler avec des délinquants (potentiels) pour s'attaquer à la « demande », il existe toujours un risque que des individus persistent à trouver de nouveaux moyens d'accéder à ces images et d'échapper à la détection. L'importance d'équilibrer les efforts entre « l'offre » et « la demande » est illustrée par une initiative actuelle de l'IWF. Responsable de la suppression de 153 600 pages Web d'abus sexuels sur enfants rien qu'en 2020, cette organisation s'est associée à la Fondation Lucy Faithfull pour développer le chatbot Rethink, avec le soutien de End Violence Partnership. Cet outil interpellera les utilisateurs montrant des signes de recherche de matériels d'abus sexuels d'enfants et les orientera vers des services d'assistance pour essayer de les dissuader d'agir avant qu'ils ne commettent une infraction<sup>256</sup>. Les initiatives de dissuasion sont également importantes d'un point de vue sociétal plus large, parce qu'« elles sont axées sur le changement de comportement des adultes », et non des enfants, et fournissent ainsi « un message important sur les personnes auxquelles incombe la responsabilité de prévenir les violences sexuelles infligées aux enfants »<sup>257</sup>.

## SUOJELLAAN LAPSIA RY: PROJET REDIRECTION

Suujellaan Lapsia Ry est une organisation non gouvernementale finlandaise qui contribue à protéger les enfants dans tous les milieux grâce à des programmes de défense, de recherche et de formation<sup>258</sup>.

Son projet ReDirection, soutenu par le End Violence Partnership, a débuté en septembre 2020 et se terminera en septembre 2022. Il s'agit d'une étude visant à recueillir de l'information afin de guider le développement de nouveaux moyens plus efficaces de décourager et d'éliminer la délinquance. L'étude comporte l'envoi d'une enquête de 30 questions, intitulée « Aidez-nous à vous aider », via Ahmia, le moteur de recherche du Dark Web qui traite environ 20 000 recherches par jour. L'enquête a été automatiquement publiée en réponse à plus de 20 000 recherches de matériels d'abus sexuels d'enfants dans un délai de trois mois. Plus de 3 100 questionnaires remplis ont été retournés.

Sur la base des résultats de cette étude, Suojellaan Lapsia prévoit de concevoir un nouveau programme d'auto-assistance pour les personnes qui recherchent et consultent du matériels d'abus sexuels d'enfants. L'objectif est d'identifier celles qui risquent de commettre des agressions et de les orienter vers des services d'aide et d'accompagnement.

Il sera essentiel d'approfondir notre compréhension des facteurs qui conduisent à la consultation de matériels d'abus sexuels d'enfants afin d'assurer une réponse efficace. Dans ce chapitre, deux motivations pertinentes ont été explorées: l'attirance sexuelle pour les enfants et la désensibilisation causée par une exposition habituelle à un contenu sexuel déviant. Même les interventions de dissuasion hautement efficaces sont peu susceptibles de décourager les individus les plus déterminés. D'où l'importance de développer des capacités de répression pour identifier les infractions persistantes et potentiellement sophistiquées. De même, il n'est sans doute ni approprié ni faisable de rechercher une résolution, par le biais de la justice pénale, du nombre croissant de délits de consultation de matériels d'abus sexuels d'enfants dus à la désensibilisation et la désinhibition en ligne.

# Agressions

## Partage et/ou stockage de matériel d'abus sexuels d'enfants

Le volume de matériels d'abus sexuels d'enfants disponible en ligne est en progression. Les méthodes de partage et de stockage du contenu évoluent.

De 2019 à 2020, le nombre de signalements de matériels d'abus sexuels d'enfants sur le service CyberTipline du NCMEC a augmenté globalement de 63%<sup>259</sup>. Au cours de la même période, l'IWF a également noté une augmentation de 16% des signalements confirmés sur ce type de matériel à la fois sur le Web de surface et le Dark Web.

Ce chiffre comprend les signalements reçus de membres du public et les découvertes faites par l'équipe de l'IWF par le biais d'une recherche active sur Internet. De telles données semblent indiquer que le volume de matériels d'abus sexuels d'enfants disponible en ligne progresse<sup>260</sup>.

Globalement, une grande partie des signalements concerne le partage répété de matériel « connu » (par opposition au matériel de « première génération » – voir les définitions ci-dessous). INHOPE, le réseau international de services de signalement, estime que 60% du contenu porté à leur attention en 2020 était du matériel « connu »<sup>261</sup>.

### Matériel « connu » et matériel de « première génération »

Le matériel d'abus sexuels d'enfants « connu » est le contenu ayant déjà été détecté et classé par les services de répression et/ou les modérateurs. Le matériel de « première génération » est un contenu « nouveau » qui n'a encore jamais été détecté ou classé.

Les vidéos représentent une fraction croissante du contenu détecté: le nombre de fichiers vidéo signalés au NCMEC a été multiplié par dix entre 2017 et 2020 (figure 14). Au cours de la même période, le nombre de fichiers image a doublé. Étant donné que de nombreux services de police et organismes de recueil des signalements ne disposent pas d'une bande passante suffisante pour traiter les images, cette tendance

pourrait entraver la détection, à moins que les capacités ne soient améliorées, sachant notamment que la capacité de stockage sur les appareils continue d'augmenter<sup>262</sup>.

Les hébergeurs d'image sont le type de site le plus couramment utilisé pour partager du matériel d'abus sexuels d'enfants<sup>264</sup>. Cela englobe les plateformes de réseaux sociaux qui sont souvent utilisées pour diffuser du matériel via de faux comptes rapidement supprimés par la suite<sup>265</sup>. Actuellement, il n'existe pas de mécanisme officiel et établi permettant aux plateformes de partager légalement les identifiants associés à ces comptes. Cela permet aux délinquants de passer librement d'une plateforme à une autre et d'un service à un autre, et d'opérer ainsi avec une impunité relative<sup>266</sup>.

L'utilisation de « services cachés » pour distribuer du matériel d'abus sexuels d'enfants a augmenté de 155% entre 2019 et 2020<sup>267</sup>. Il s'agit de sites Web hébergés dans un réseau proxy (tel que « Tor » – voir définition du glossaire), de façon à empêcher leur localisation<sup>268</sup>.

Bien que certains agresseurs continuent à amasser du matériel sur des appareils tels que des ordinateurs portables, des téléphones mobiles et des clés USB<sup>269</sup>, les faits montrent un déclin des collections personnelles, les délinquants privilégiant un accès au contenu à la demande via l'utilisation d'« hébergeurs de fichiers »<sup>270</sup>, c'est-à-dire de services Internet qui permettent aux utilisateurs de télécharger des fichiers pour y accéder à distance<sup>271</sup>. Des liens vers des fichiers contenant du matériel d'abus sexuels d'enfants sont affichés sur plusieurs sites et sont souvent utilisés dans le cadre du partage pair-à-pair.

Cela crée une multitude de défis pour les forces de l'ordre. Le matériel est souvent publié et hébergé dans différents pays, ce qui complique la collecte de données probantes<sup>272</sup>. Le volume de contenu détenu par un délinquant était historiquement l'un des nombreux facteurs utilisés pour évaluer le niveau de risque qu'il représentait, mais ce n'est plus toujours significatif<sup>273</sup>.



# Les applications de partage sur le cloud alimentent l'explosion des interactions des utilisateurs avec les contenus malveillants.



Les populations de délinquants ont fini par s'appuyer sur la facilité d'utilisation, la sécurité et la confidentialité des applications de partage de fichiers sur le cloud pour stocker et distribuer des images et des vidéos illégales. Le stockage dans le cloud permet de partager du matériels d'abus sexuels d'enfants par la simple publication d'un lien sur un forum, sur une plateforme ou via une messagerie directe, ce qui permet d'atteindre un plus grand nombre de délinquants plus rapidement.

L'analyse de Crisp montre que les cas d'implication d'utilisateurs dans du contenu d'abus sexuels d'enfants malveillant ou d'interaction avec celui-ci ont explosé de plus de 5,5 millions au premier trimestre 2020, en forte progression à près de 20 millions au premier trimestre 2021.

Sur les cinq trimestres de janvier 2020 à mars 2021, Crisp a évalué 1 340 éléments contenant des liens de partage de contenu

jugé à haut risque du fait de leur contexte et des communautés dans lesquels ils avaient été partagés. Lorsqu'un lien malveillant figurait dans le contenu, le nombre d'interactions variait de 20 à 12 746 dans les cas extrêmes. Le partage dans différents forums et lieux à l'échelle mondiale a considérablement augmenté le nombre total d'interactions des utilisateurs avec de tels liens.

Les délinquants utilisent en général le partage de fichiers sur le cloud pour échanger efficacement des images et des vidéos avec d'autres délinquants, qui sont des contacts connus ou nouveaux. Pour garantir que le contenu reste accessible aussi longtemps que possible, les plus déterminés utilisent simultanément plusieurs plateformes sur le cloud. La véritable nature des liens malveillants est masquée derrière un écran de fumée constitué par des références à d'autres activités moins illégales ou à des utilisations légitimes de partage de fichiers pour échapper à la détection.

Figure 15: Interactions des utilisateurs avec du contenu malveillant.

## Interactions des utilisateurs - Par trimestre

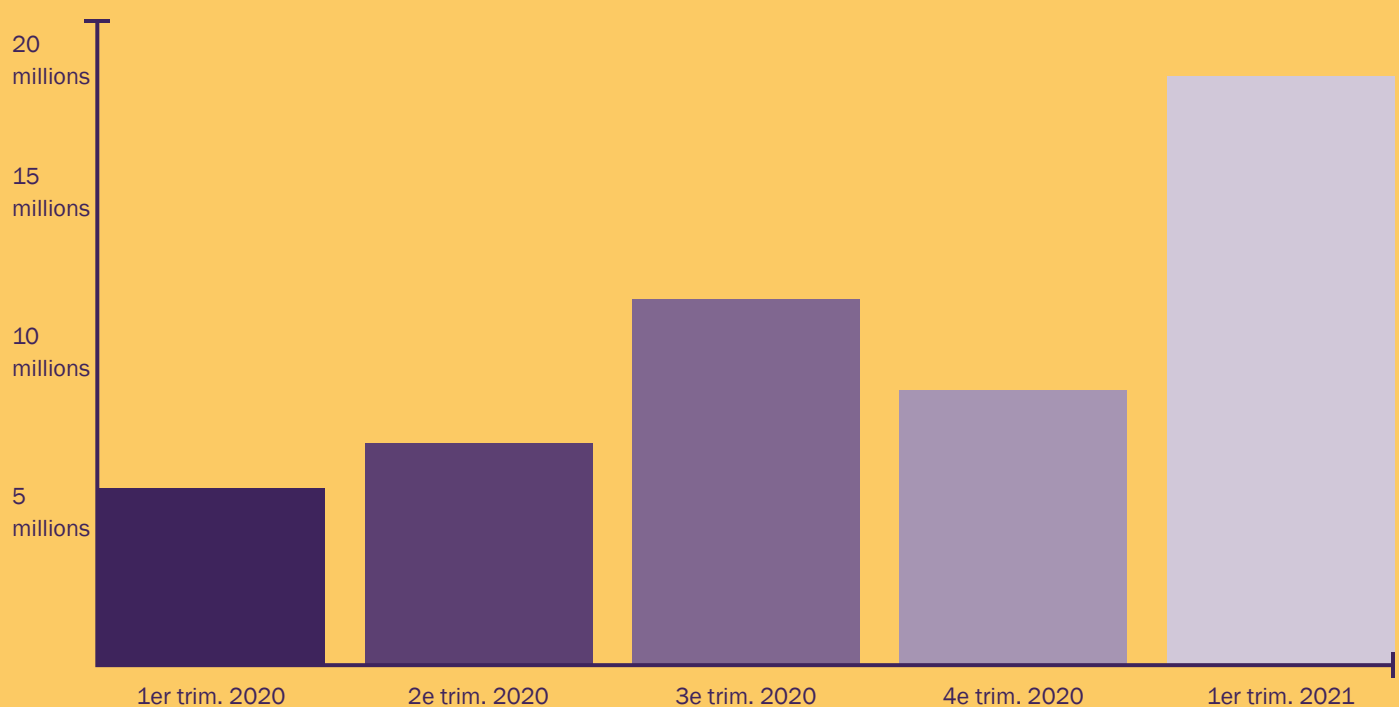


Figure 14: Augmentation du matériels d'abus sexuels d'enfants basé sur des images par rapport aux vidéos. Publié avec la permission du NCMEC <sup>263</sup>.

Données du NCMEC sur les tendances : hausse des images et vidéos d'abus sexuels d'enfants		
Année	Images	Vidéos
2020	33,6 millions	31,6 millions
2019	27,7 millions	41,2 millions
2018	23,2 millions	22,2 millions
2017	17,0 millions	3,4 millions

### Le partage de contenu de façon répétée aggrave les dommages causés aux enfants victimes d'agressions sexuelles.

Une proportion significative des signalements de matériels d'abus sexuels d'enfants provient de ce repartage d'images « connues ». Selon Facebook, plus de 90% de ses signalements au NCMEC en octobre et novembre 2020 concernaient des partages et repartages de contenus déjà détectés<sup>274</sup>. D'après une étude portant sur un échantillon de 2 598 signalements effectués auprès du NCMEC entre 2011 et 2014, les images avaient été « activement échangées » (c'est-à-dire qu'elles avaient été signalées au NCMEC cinq fois ou plus) par un seul délinquant avec une seule victime dans 7% des cas, et par plusieurs victimes et/ou délinquants dans 12% des cas<sup>275</sup>. Dans toutes les situations, la répétition du partage « aboutit à victimiser de nouveau et donc à aggraver les dommages psychologiques causés aux personnes agressées » ; elle empêche souvent la cessation des abus, même dans les cas où le délinquant est pris et sanctionné<sup>277</sup>. À mesure que le repartage de contenu se développe en ligne, le recours aux politiques d'acceptation des notifications par les victimes (telles qu'elles existent aux États-Unis) sera de plus en plus essentiel pour assurer que les agressions ne soient pas involontairement réitérées à chaque fois que des images des survivants seront redécouvertes par la police ou les agences de recueil des signalements<sup>278</sup>.

Parmi les autres problèmes liés au partage répété de contenu, citons le harcèlement et la traque de victimes spécifiques, une activité qui offre également aux délinquants la possibilité de communiquer avec des personnes partageant les mêmes idées.

**Dans tous les cas, la répétition du partage « aboutit à victimiser de nouveau et donc à aggraver les dommages psychologiques causés aux personnes agressées » ; elle empêche souvent la cessation des abus, même dans les cas où le délinquant est pris et sanctionné.**

Selon Facebook,

**90%**

de ses signalements auprès du NCMEC entre octobre et novembre 2020 concernaient des partages ou repartages de contenus déjà détectés.

Une étude des signalements effectués auprès du NCMEC entre 2011 et 2014 montre qu'un échantillon de

**2 598**

images avaient été « activement échangées » (c'est-à-dire signalées auprès du NCMEC cinq fois ou plus).

# Les agresseurs traumatisent à nouveau les survivants en utilisant de faux profils.



Employant une tactique qui revictimise les enfants ayant survécu à des agressions sexuelles, les délinquants créent de faux profils en ligne qui s'approprient l'identité de survivants connus. Ces comptes frauduleux, qui adoptent en général le nom des survivants et présentent des images non préjudiciables au niveau du compte/profil, apparaissent sur plusieurs réseaux sociaux du Web.

Les comptes sont utilisés par des communautés de délinquants pour établir des liens avec d'autres acteurs partageant leurs idées, principalement pour échanger des coordonnées. Cela peut aboutir à l'échange de tactiques d'exploitation, « techniques de dissimulation » et matériels d'abus sexuels d'enfants dans un espace en ligne perçu comme « sûr ».

La plupart des délinquants utilisent ces comptes pour faire connaître leurs intérêts et préférences, et cautionner des sites commerciaux qui distribuent des images pornographiques. Confirmant une tendance inquiétante,

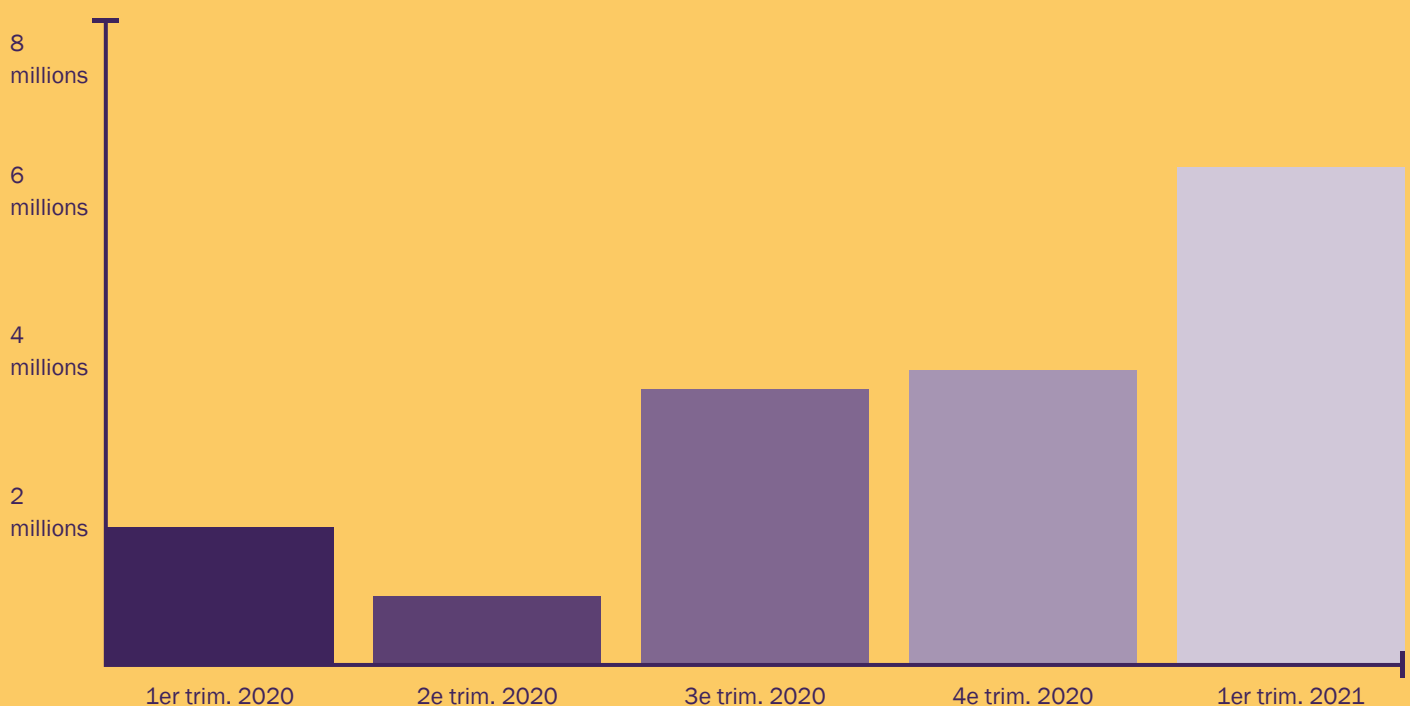
Crisp a noté un triplement des interactions des utilisateurs avec de faux profils entre le premier trimestre 2020 et le premier trimestre 2021.

Par exemple, de janvier 2020 à mars 2021, Crisp a identifié 3 324 contenus faisant référence à des survivants connus ou à des sites marchands. En moyenne, chaque contenu préjudiciable a généré plus de 2 000 interactions (J'aime, commentaires, etc.), créant une démultiplication et atteignant beaucoup plus de délinquants.

La majorité des comptes comportaient des discussions de délinquants et la confirmation de la consommation de matériels d'abus sexuels d'enfants. La plupart du contenu auquel il était fait référence était lié à des délits remontant à plus de dix ans avant la création des faux profils. Cette mémoire des agressions sexuelles passées a pour effet de perpétuer le traumatisme des survivants qui, à chaque fois, n'ont plus le contrôle sur leur identité telle que décrite sur les réseaux sociaux.

Figure 16: Interactions des utilisateurs avec du contenu faisant référence à des survivants connus ou des sites marchands.

## Interactions des utilisateurs - Par trimestre



## NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC): l'histoire d'Ella

Ella\* a été agressée sexuellement par un membre de sa famille dès l'âge de cinq ans et pendant une période de sept ans. Son agresseur prenait des images et des vidéos des agressions et les diffusait en ligne. Le NCMEC a repéré le lieu de l'agression dans une zone de l'ouest des États-Unis et a transmis l'affaire aux autorités locales. La police a localisé et sauvé Ella ; quant au contrevenant, il a été reconnu coupable et condamné.

Bien que le délinquant soit maintenant en prison, les images et vidéos d'Ella circulent toujours et d'autres délinquants continuent de la harceler en ligne. La personne qui la soigne a décrit le traumatisme créé par ces nouveaux partages: « On a l'impression que lorsque le délinquant est en prison, c'est fini mais ce n'est pas le cas... au début, j'ai été curieusement reconnaissante pour les photos parce que c'est ce qui avait permis de l'attraper. Mais les images sont toujours là, elles ne partent pas. Des dizaines de milliers de personnes ont vu Ella... encore 10 ans plus tard ».

Au fil des années, elle a reçu des milliers de notifications de cas impliquant des images et vidéos d'elle-même en tant que victime de la part du gouvernement. Même à l'âge adulte, cette revictimisation a rendu nécessaire pour Ella de suivre une thérapie continue.

Elle s'appuie maintenant sur son expérience pour aider les autres. Elle est consultante pour les survivants et contribue à orienter le développement des ressources d'assistance du NCMEC et à créer de nouveaux services de programme pour les autres survivants.

Le National Center for Missing and Exploited Children (NCMEC) est un organisme privé à but non lucratif. Sa mission est de retrouver les enfants disparus, de lutter contre l'exploitation sexuelle des enfants et d'empêcher la victimisation des enfants.

\* Pseudonyme

Facebook a analysé les cas de partage de contenu de 2019 à mi-2020 et a conclu que 75% d'entre eux étaient « non malveillants ». Selon la taxonomie de Facebook, ce partage est soi-disant motivé par l'indignation, une tentative d'humour ou des raisons d'autodéfense<sup>279</sup>. Une plus grande transparence dans la classification des partages « non malveillants » et des taxonomies appliquées par d'autres plateformes seraient utiles pour éclairer les stratégies visant à freiner cette tendance. Une approche proactive des prestataires de services en ligne est essentielle.

**pour gérer ces comportements et atténuer le risque associé de normalisation, voire banalisation, des abus sexuels sur les enfants en ligne. Le matériels d'abus sexuels d'enfants est distribué en vue d'un profit financier. Ce type de partage crée des difficultés de détection spécifiques.**

Selon l'IWF, alors que la proportion de pages Web commerciales contenant du matériels d'abus sexuels d'enfants a légèrement diminué (- 4%) par rapport à l'année qui précède<sup>280</sup>, la majorité (61%) des domaines analysés en 2020 étaient de nature commerciale<sup>281</sup>. L'IWF a continué à observer les nouveaux moyens de monétiser le contenu, tels que les programmes d'affiliation qui permettent aux éditeurs de gagner de l'argent à chaque fois qu'une personne clique sur un lien pour accéder à du matériels d'abus sexuels d'enfants<sup>282</sup>.

Il y a également eu une augmentation spectaculaire de l'utilisation enregistrée des cryptomonnaies pour acheter ce type de matériel. La valeur totale des paiements en Bitcoin et Ethereum aux adresses liées aux fournisseurs de ces contenus était de 930 000 USD en 2019, soit une augmentation de 212% par rapport à 2017<sup>283</sup>. Cette tendance est corrélée avec l'accroissement de l'utilisation de services marchands cachés pour accéder au contenu. La part de ces services a augmenté depuis 2016<sup>284</sup> et les cryptomonnaies sont le seul mode de paiement qu'ils acceptent<sup>285</sup>.

Le partage commercial peut poser des difficultés spécifiques, car les distributeurs déploient souvent des tactiques pour contrecarrer les tentatives de détection et de suppression des images. En 2020, une augmentation des sites marchands déguisés a été observée. Ils échappent à la détection en n'affichant d'images illégales que lorsque l'accès au site a été effectué par un « chemin numérique » spécifique de liens provenant d'autres sites. D'autres sites marchands utilisent des techniques telles que le « saut au domaine de premier niveau » pour survivre en ligne après la suppression du site initial. C'est ce qui se passe quand un site modifie son nom de domaine tout en conservant son nom de marque pour que les utilisateurs puissent toujours le localiser<sup>286</sup>.

## Il faudra innover davantage et adopter plus largement les outils pour détecter les contenus et endiguer le repartage.

Deux techniques liées, appelées « hachage » et « correspondance de hachage », rendent possible une détection efficace du matériels d'abus sexuels d'enfants « connu ». Ces techniques ont considérablement accéléré l'identification de ce matériel et sa suppression d'Internet.

### Hachage et correspondance de hachage

Le « hachage » est un processus utilisé pour transformer des données de toute taille en données de longueur fixe beaucoup plus courtes. La séquence la plus courte contient les données d'origine et devient la signature unique du fichier ou sa valeur de hachage.

La « correspondance de hachage » est un processus par lequel les hachages de contenus d'abus sexuels d'enfants connus, figurant dans les bases de données, sont comparés au hachage du contenu nouvellement découvert afin de déterminer si celui-ci a déjà été signalé aux autorités. Si c'est le cas, le processus de suppression du contenu est généralement simplifié et souvent automatisé<sup>287</sup>.

Plusieurs bases de données existent pour faciliter la correspondance de hachage. L'une des principales est celle d'Interpol, qui comporte plus de 2,7 millions de hachages de contenus d'abus sexuels d'enfants et est utilisée par 64 forces de police dans le monde entier<sup>288</sup>. Parmi les autres utilisateurs, citons la Child Abuse Image Database au Royaume-Uni, la liste de hachage de l'IWF et le système CyberTipline du NCMEC.

Mais la correspondance de hachage présente certaines limites. Lorsque des images « connues » sont détectées, leur suppression dépend de l'identification de l'hébergeur pour émettre un avis de retrait<sup>289</sup>. Dans certains pays, le non-respect des avis de retrait est également un problème<sup>290</sup>. Une collaboration étroite et continue entre les gouvernements, le secteur et les forces de l'ordre dans le monde entier est essentielle pour assurer le maintien de l'efficacité de cet outil.

Et une adoption plus large de la technologie est indispensable pour améliorer son impact<sup>291</sup>. Bien que la majorité des participants à une enquête Alliance/Tech Coalition aient confirmé qu'ils utilisaient la correspondance de hachage à la fois des images (87%) et des vidéos (76%) pour supprimer de manière proactive le matériels d'abus sexuels d'enfants de leurs plateformes, de nombreuses organisations ne contribuent toujours pas au hachage des bases de données existantes, ni à la comparaison de celles-ci<sup>292</sup>.

La détection et la suppression basées sur le hachage pourraient être optimisées en fusionnant les listes de hachage existantes. Toutefois, tout cela est compliqué par les différences entre les façons dont les pays classent le matériel. Interpol applique une balise de référence au matériel illégal dans tous les pays, qui est utilisée par nombre de ses partenaires judiciaires<sup>293</sup>. Mais il est plus difficile de parvenir à un consensus mondial sur la classification des images de moindre gravité. Une meilleure adhésion internationale pourrait améliorer la déduplication et la détection afin de renforcer significativement l'impact global de la technologie<sup>294 295</sup>.

La détection et la suppression du matériels d'abus sexuels d'enfants de « première génération » posent une autre série de difficultés. Il existe des solutions pour détecter les contenus nouveaux, mais elles sont relativement moins matures et plus complexes sur le plan technique que les correspondances de hachage. Les « classificateurs de contenu », comme on les appelle, utilisent des algorithmes renseignés par l'apprentissage machine pour identifier et classer le matériels d'abus sexuels d'enfants. Les difficultés à estimer l'âge des enfants sur les images<sup>296</sup> et à évaluer la gravité de celles-ci font que ces systèmes ont tendance à générer un taux de faux positifs plus élevé que celui obtenu avec la correspondance de hachage, ce qui augmente le besoin de modération humaine<sup>297</sup>. Il conviendra aussi de s'employer à étudier la façon dont les classificateurs et la correspondance de hachage pourraient fonctionner efficacement avec le chiffrement de bout en bout.

### GOOGLE: CONTENT SAFETY API

La Content Safety API est un outil développé par Google et fourni gratuitement aux ONG et aux entreprises privées pour soutenir leur travail de protection des enfants. Elle utilise l'intelligence artificielle pour aider les organisations à mieux hiérarchiser les images potentiellement illicites en vue d'un examen par l'homme, si le contenu n'est pas du matériels d'abus sexuels d'enfants « connu ». L'identification plus rapide des nouvelles images augmente la vitesse à laquelle les victimes d'abus peuvent être identifiées et protégées. La hiérarchisation efficace réduit également la pression exercée sur les modérateurs et les évaluateurs.

Cet outil a déjà traité plus de deux milliards d'images, aidant des entreprises comme Yubo, Plugin et Facebook, ainsi que des ONG comme Safernet Brésil, à améliorer la détection du matériels d'abus sexuels d'enfants et son signalement.

# 06 Agressions

## Contenu à caractère sexuel « autoproduit » par les enfants

Le volume de contenu à caractère sexuel « autoproduit » par les enfants a augmenté pendant la pandémie de COVID-19.

Le matériel « autoproduit » par les enfants comprend une proportion croissante de contenu d'abus sexuels d'enfants. Cela crée des défis complexes pour les responsables politiques et exige une réponse nuancée.

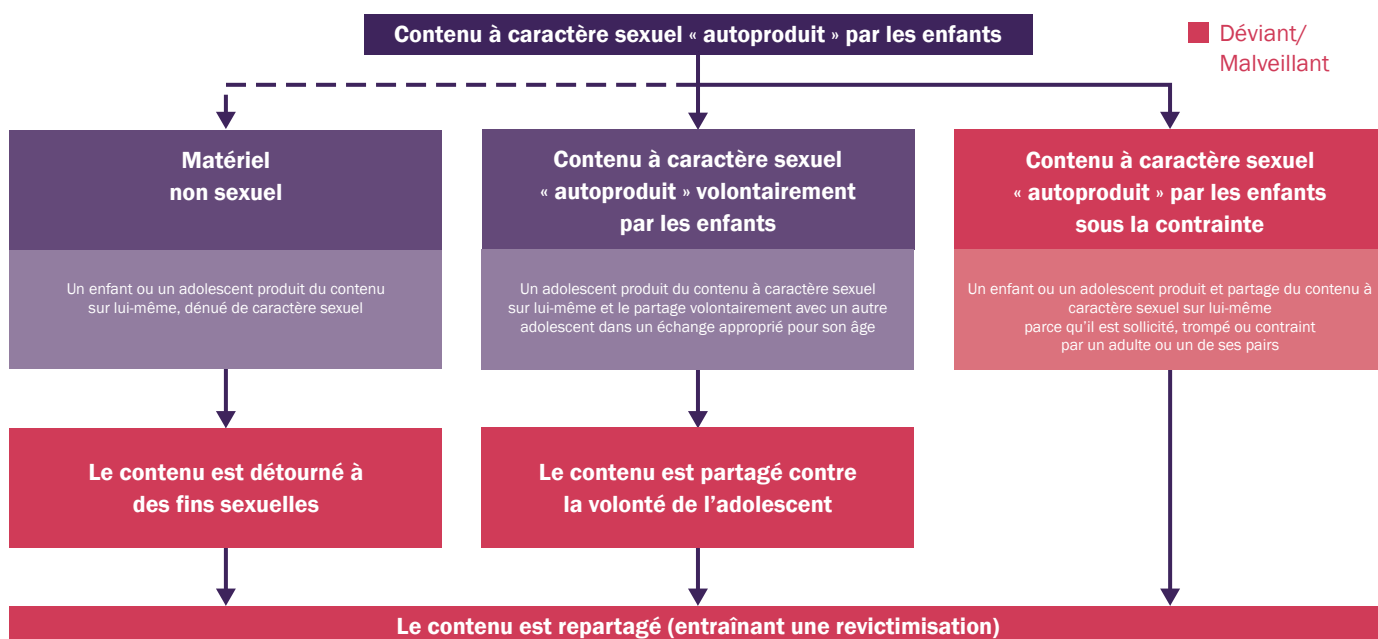
Dans son rapport annuel 2012, l'IWF a présenté une « brève étude » sur le contenu « autoproduit »<sup>298</sup>. En 2017, l'ECPAT l'a également décrit comme une « tendance actuelle », en attribuant le volume croissant de ce matériel à la marchandisation d'images « récemment produites et encore jamais vues », ce qui en a fait une « valeur » précieuse pour les délinquants<sup>299</sup>.

Récemment, le volume du matériel « autoproduit » a augmenté de façon considérable.

L'IWF a reçu 68 000 signalements de contenu à caractère sexuel « autoproduit » en 2020, soit une augmentation de 77% par rapport à 2019. Dans l'ensemble, ce contenu représentait 44% de tous les signalements traités par l'IWF en 2020<sup>300</sup>.

Cette escalade a été en partie attribuée au « raz-de-marée » créé par la pandémie de COVID-19: les enfants passent plus de temps en ligne et les opportunités réduites de commettre des abus « physiques » alimentent la délinquance et la demande d'images en ligne<sup>301</sup>.

Figure 17: Principales catégories de contenu à caractère sexuel « autoproduit » et agressions liées.



Les causes de l'« autoproduction » sont complexes et variées.

Il existe trois grandes catégories de matériel « autoproduit » (voir figure 17):

- Le matériel non pornographique est un contenu « autoproduit » qui n'est pas à caractère sexuel, mais qui est détourné et utilisé en relation avec l'exploitation et les abus sexuels en ligne envers les enfants<sup>302</sup>. Bien que les victimes n'en soient pas conscientes, ce matériel est préjudiciable essentiellement parce qu'il facilite l'activité des délinquants. Dans certains cas, les victimes subissent également un préjudice direct causé par la manipulation des images par les délinquants afin qu'elles semblent présenter un caractère sexuel, puis par le chantage exercé auprès des enfants en les menaçant de les partager<sup>303</sup>.
- Le matériel volontairement « autoproduit » est généralement partagé par les adolescents entre eux. Cette catégorie ne couvre que l'« autoproduction » par des adolescents, parce que les enfants plus jeunes ne peuvent pas donner leur consentement. Par conséquent, l'« autoproduction » qui les concerne ne peut être considérée comme « volontaire ». Dans de tels scénarios, le mal est généralement fait lorsque les images sont (re)partagées contre la volonté des jeunes. Sur 39 études différentes menées auprès de 110 380 participants âgés de 12 à 17 ans, 12% ont signalé la transmission d'une image à caractère sexuel « autoproduite » sans leur consentement<sup>304</sup>. Dans l'étude d'Economist Impact, commanditée en même temps que ce rapport, 29% des personnes interrogées ont déclaré qu'une personne avait partagé des images et/ou des vidéos sexuellement explicites sans leur autorisation. Le partage non sollicité de matériel volontairement « autoproduit » peut également causer un préjudice aux destinataires de ce contenu<sup>305</sup>.
- L'« autoproduction sous la contrainte » est la sollicitation d'enfants pour leur faire créer des images pornographiques. Cette pratique a été liée au « capping »<sup>306</sup>. Les enfants concernés par une « autoproduction sous la contrainte » risquent de ne pas se percevoir comme des victimes et peuvent éventuellement considérer leurs propres actions comme délibérées.

Les différentes formes d'« autoproduction » créent un défi pour ceux qui ripostent à cette menace. Bien que le contenu d'une image ou d'une vidéo puisse correspondre à la définition juridique de « matériels d'abus sexuels d'enfants » et, par conséquent, permettre d'invoquer certains processus juridiques une fois découvert, l'intention derrière la création ou le partage des images peut être floue. Il est essentiel de comprendre le contexte de la production et/ou du partage de ce type de contenu pour s'assurer d'adapter correctement la riposte. Par conséquent, une approche au cas par cas est toujours nécessaire.

## INTERNET WATCH FOUNDATION Contenu à caractère sexuel « autoproduit » par des fratries

L'Internet Watch Foundation (IWF) est un organisme de protection de l'enfance qui utilise la technologie pour rechercher le matériels d'abus sexuels d'enfants sur Internet en vue de le se supprimer<sup>307</sup>. En 2020, l'IWF a noté une augmentation alarmante du volume de matériel « autoproduit » en ligne<sup>308</sup>. Dans celui-ci, les analystes ont observé une tendance particulièrement inquiétante chez les délinquants. En effet, ceux-ci ont tendance à inciter sournoisement les enfants à impliquer d'autres enfants dans leur « autoproduction » de matériels d'abus sexuels d'enfants.

L'analyse des images sexuelles « autoproduites » signalées à l'IWF entre septembre et décembre 2020 a révélé ce qui suit:

# 511

images et vidéos représentaient des fratries

# 65%

d'entre elles montraient un ou deux enfants ayant un contact sexuel direct avec un autre

# 46%

de ce matériel a été classé comme contenu de Catégorie A, incluant les formes les plus graves d'abus sexuels

Dans de nombreux cas, les enfants avaient été manipulés ou contraints par des adultes à diffuser en direct des activités sexuelles, et les vidéos et captures d'écran qui en avaient résulté avaient été partagées sur diverses plateformes Web. Certains adultes se présentaient comme des enfants et parfois les abus prenaient la forme d'un jeu ou d'un « défi ». Les enfants concernés ont rarement démontré une compréhension de la nature sexuelle de ce qu'on leur demandait de faire.

Bien que les données indiquent que le partage d'images sexuelles est une pratique plutôt courante chez les jeunes (voir figure 18), certains enfants sont plus susceptibles que d'autres d'être incités à s'y prêter, ce qui peut accroître le risque pour eux de faire l'objet d'une coercition et/ou d'un partage d'images non consensuel.

## HAMOGELO: l'histoire de Maria

Maria\* a 15 ans et vit en Grèce. Elle a commencé à parler à Yannis\*, un jeune homme de 20 ans, sur une plateforme de rencontre. Elle avait utilisé la plateforme par curiosité et par ennui: les restrictions imposées par les confinements dus à la COVID-19 ne lui permettaient pas d'aller à l'école ni de participer à ses activités de plein air habituelles.

Yannis lui avait posé des questions au sujet de la vie durant la pandémie, l'avait écoutée et semblait partager ses sentiments. Il lui parlait tous les jours et ils se sont progressivement rapprochés.

Puis Yannis a fini par contraindre Maria à lui envoyer des images sexuelles produites par elle-même. Il l'a convaincue que c'était une nouvelle étape dans leur « relation » et que ce serait un secret entre eux. Au fil du temps, il a commencé à lui demander d'en faire plus, notamment de créer des vidéos.

Maria a essayé de refuser, mais Yannis l'a menacée alors de publier ses photos sur les réseaux sociaux. Désespérée, elle a cherché de l'aide en ligne et a trouvé la ligne d'assistance 1056 de Hamogelo.

Ce service lui a apporté un soutien et des conseils de façon anonyme et l'a aidé à parler de ce problème à ses parents. Ensemble, ils ont contacté la ligne d'assistance et l'affaire a été transmise à la Division de cybercriminalité de la police hellénique, qui a pu procéder à l'arrestation de Yannis.

Hamogelo ou « Le sourire de l'enfant » est une organisation grecque qui soutient les enfants confrontés à la violence, aux abus, à l'extorsion, à la pauvreté et aux problèmes de santé. À ce jour, elle a aidé plus de 1,7 million d'enfants et de familles.

\*Pseudonymes

Une étude récente révèle que les adolescents flamands s'identifiant comme LGBTQ+ sont davantage poussés à partager des images pornographiques que leurs pairs hétérosexuels<sup>309</sup>. Une autre étude sur « les adolescents, le sexting et les risques » réalisée par une association caritative britannique, Internet Matters, a également montré que les « groupes vulnérables » (enfants ayant un ou plusieurs handicaps physiques, mentaux ou sociaux) sont beaucoup plus susceptibles d'être soumis à des pressions ou à des chantages pour les inciter à partager des images d'eux-mêmes nus<sup>310</sup>. Le harcèlement sexuel sous la forme de demandes persistantes de matériel « autoproduit » n'est apparemment pas rare dans certains pays. Dans une enquête menée par l'Office for Standards in Education, Children's Services and Skills (OFSTED) au Royaume-Uni, sur un échantillon de 900 jeunes, 80% des filles avaient déclaré avoir été contraintes de partager des images à caractère sexuel d'elles-mêmes « souvent » ou « parfois ». Parmi les autres causes contribuant à l'autoproduction, nous pouvons citer les antécédents d'abus, la participation à des « comportements plus risqués en ligne et dans le monde réel », et l'utilisation fréquente de forums de discussion en ligne<sup>311 312</sup>.

Selon l'IWF, les filles au début de l'adolescence sont beaucoup plus susceptibles d'apparaître dans cette forme d'images: 95% du contenu sexuel « autoproduit » signalé à cet organisme en 2020 présentait des filles âgées de 11 à 13 ans<sup>313</sup>. Toutefois, d'autres études suggèrent qu'une proportion égale ou supérieure de garçons « autoproduisent » du contenu de ce type:

- Dans une enquête américaine menée auprès de 1 000 jeunes âgés de 13 à 17 ans, la proportion de garçons ayant partagé des images de leur nudité était de 1 sur 10 (alors que, pour les filles, le chiffre était de 1 sur 5)<sup>314</sup>.
- Une enquête en ligne menée auprès de 1 001 jeunes âgés de 13-17 ans au Royaume-Uni montre un nombre égal de garçons et de filles ayant pris des photos d'eux-mêmes complètement nus<sup>315</sup>.
- Enfin, dans une enquête menée auprès de 500 jeunes âgés de 13 à 24 ans et vivant dans la vallée de Katmandou au Népal, 18% des garçons et 5,2% des filles ont déclaré prendre des photos d'eux-mêmes nus<sup>316</sup>.

Il faudrait mener davantage d'études pour comprendre le rôle du genre comme facteur de risque, et comment cela peut varier selon les différents types d'agressions liées au contenu à caractère sexuel « autoproduit » par les enfants (par exemple, la production forcée par rapport à la « production volontaire »). Les autres facteurs de risque courants favorisant l'« autoproduction » sont liés aux caractéristiques de l'utilisation d'Internet par les enfants. L'usage croissant des appareils mobiles<sup>317</sup> limite la possibilité d'une surveillance parentale. Ceci conjugué à la facilité d'accès aux plateformes et aux contenus destinés aux adultes (en raison de la non-vérification de l'âge ou de contrôles facilement contournés)<sup>318</sup> permet facilement d'imaginer comment les conditions d'« autoproduction » de matériels d'abus sexuels d'enfants peuvent être réunies, même en l'absence d'autres causes contribuant à ce risque.



### « L'autoproduction » en échange d'un paiement risque d'augmenter à cause de la pauvreté provoquée par la COVID-19.

Elle est commercialement motivée lorsque les enfants créent des images ou des vidéos sexuelles d'eux-mêmes en échange d'un paiement. Les signalements d'« autoproduction » commercialement motivée sont en train d'émerger partout dans le monde. Aux Philippines, les autorités ont découvert des cas d'adolescents qui créent des groupes sur des plateformes sociales pour vendre des images et des vidéos à caractère sexuel « afin de financer des dépenses de formation en ligne ». Un de ces groupes a même réuni 7 000 membres avant d'être supprimé<sup>319</sup>. Au Cambodge, certains jeunes (principalement des filles) utilisent leur contenu sexuel pour vendre des produits cosmétiques en ligne. Les enquêtes menées auprès de jeunes Cambodgiens montrent que cette activité peut aboutir à de graves agressions sexuelles<sup>320</sup>. Le NCMEC a mis en évidence des cas d'enfants disparus dont on a découvert plus tard qu'ils vendaient leur contenu sexuel sur des plateformes d'abonnés, et pour lesquels des preuves de l'existence d'un lien avec la traite et l'exploitation organisée d'enfants ont été établies<sup>321</sup>.

Quelles que soient les circonstances, tous les actes d'« autoproduction » à caractère commercial mettent certainement les enfants en danger, et le matériel ainsi créé est très probablement illégal. La question exige une réponse urgente et réfléchie de la part des décideurs politiques. L'enquête de NetClean menée en 2020 auprès des forces de l'ordre mondiales révèle que certains services ont déjà observé une augmentation de l'« autoproduction » « en échange d'argent » pendant la pandémie. D'autres prédisaient que cette tendance se maintiendrait à mesure de l'aggravation des difficultés économiques, car c'était un moyen pour les enfants de « gagner de l'argent pour s'acheter des choses qu'ils ne pouvaient pas s'offrir autrement »<sup>322</sup>.

### Les dangers causés par le matériel « autoproduit » englobent également le harcèlement, l'intensification du partage de ce matériel et la stigmatisation des victimes.

L'IWF a constaté certains cas de délinquants qui, après avoir vu du contenu autoproduit, tentaient d'identifier et de suivre les victimes, dans le but des obliger à en créer encore davantage<sup>323</sup>. Dans d'autres scénarios, on peut connaître les auteurs initiaux de ces actes, comme dans le cas d'« abus physiques », car ils sont souvent commis par des « personnes dont dépendent les enfants et sur lesquelles ils comptent »<sup>324</sup>. Ces deux facteurs peuvent créer un sentiment d'inéluctabilité autour de l'abus, qui est amplifié lorsque le contenu est partagé de façon répétée. En 2014, l'IWF a évalué plus de 3 800 images et vidéos pornographiques « autoproduites » et a constaté que 90% d'entre elles avaient été « recueillies à partir du site de téléchargement initial, puis redistribuées sur des sites tiers »<sup>325</sup>.

Les dommages causés par le matériel « autoproduit » sont susceptibles d'être exacerbés par une tendance à blâmer les victimes. Selon une enquête de Thorn, 60% des enfants accusent la victime lorsque du matériel « autoproduit » est repartagé, et 55% des aidants estiment également que la victime est principalement ou exclusivement à blâmer dans ce cas<sup>326</sup>. De telles attitudes nuisent à la divulgation et au signalement des agressions en alimentant les stigmates qui empêchent les enfants de se manifester.

### Les initiatives de signalement et les solutions technologiques peuvent freiner la montée en puissance du matériel « autoproduit », mais la prévention exige une approche plus nuancée.

La campagne « Report Remove », lancée au Royaume-Uni en 2020, vise à permettre aux enfants de signaler de manière anonyme du matériel « autoproduit » et de demander son retrait<sup>327</sup>. De telles initiatives réduisent les obstacles à la divulgation. Les contrôles au niveau des appareils qui empêchent les enfants de capturer des images et des vidéos à caractère sexuel peuvent également être un « expédient » efficace pour freiner l'augmentation de l'« autoproduction ». « SafeToWatch », un outil d'analyse des images et vidéos pour déceler les menaces en est un bel exemple (voir l'étude de cas au verso). De telles solutions ont une incidence sur le droit des enfants à la vie privée, qui devra être soigneusement examiné afin de favoriser une adoption large et un déploiement efficace.

Une prévention soutenue à long terme nécessitera des approches réfléchies, fondées sur les expériences complexes des enfants et des jeunes expérimentant avec la découverte de soi à l'ère numérique. Étant donné que le partage d'images sexuelles « autoproduites » n'est pas rare et ne cause pas toujours de tort, une attention excessive aux résultats négatifs potentiels risque d'aboutir à des conseils qui seront rejetés, car ils ne correspondront pas aux expériences habituelles des jeunes<sup>328</sup>. L'éducation sera essentielle pour protéger les enfants et leur éviter de devenir des victimes de la coercition et des conséquences négatives potentielles de « l'autoproduction volontaire ». Les initiatives éducatives peuvent aussi contribuer à promouvoir un développement sexuel sain et à faire comprendre ce qu'implique le consentement<sup>329</sup>. La campagne « Send me a pic » de la National Crime Agency au Royaume-Uni, qui vise à promouvoir un dialogue constructif avec les jeunes sur le partage d'images de nus, est un exemple de ce type d'initiatives.

## SAFETONET : SAFETOWATCH

SafeToNet est une société de technologie de sécurité qui utilise l'analyse comportementale et l'intelligence artificielle pour contribuer à protéger les enfants en ligne. Selon elle, les fonctions de sécurité destinées à la protection des enfants devraient être intégrées aux technologies au niveau des terminaux et des systèmes d'exploitation.

La dernière innovation de SafeToNet est SafeToWatch, un outil d'analyse des images et vidéos pour déceler les menaces, qui peut interrompre la création de matériels d'abus sexuels d'enfants en temps réel et à la source. Il utilise plusieurs entrées, telles que l'audio et la vidéo, pour évaluer l'environnement numérique en ligne de l'enfant et applique un ensemble unique d'algorithmes pour permettre la détection en temps réel du matériels d'abus sexuels d'enfants. SafeToWatch fonctionne de la même manière, que le contenu soit diffusé en direct par un tiers ou « autoproduit » par l'enfant. La détection de telles images déclenche immédiatement le blocage des caméras et micros, ce qui peut rendre inutilisable une application ou l'appareil dans son ensemble et empêcher ainsi la prise de la photo ou de la vidéo. Les images ne sont pas conservées, ce qui préserve le droit des enfants à la vie privée. Contrairement aux outils de détection au niveau de la plateforme, cette technologie est facilement déployable dans les environnements chiffrés de bout en bout. Pour assurer la réussite de SafeToWatch et d'autres innovations similaires, un accès fiable aux données du gouvernement et des forces de l'ordre est essentiel afin d'entraîner les algorithmes et d'optimiser l'efficacité de ces solutions.

SafeToNet a acquis 77 magasins de téléphonie mobile en Allemagne pour mettre la cybersécurité à la disposition de tous<sup>330</sup>

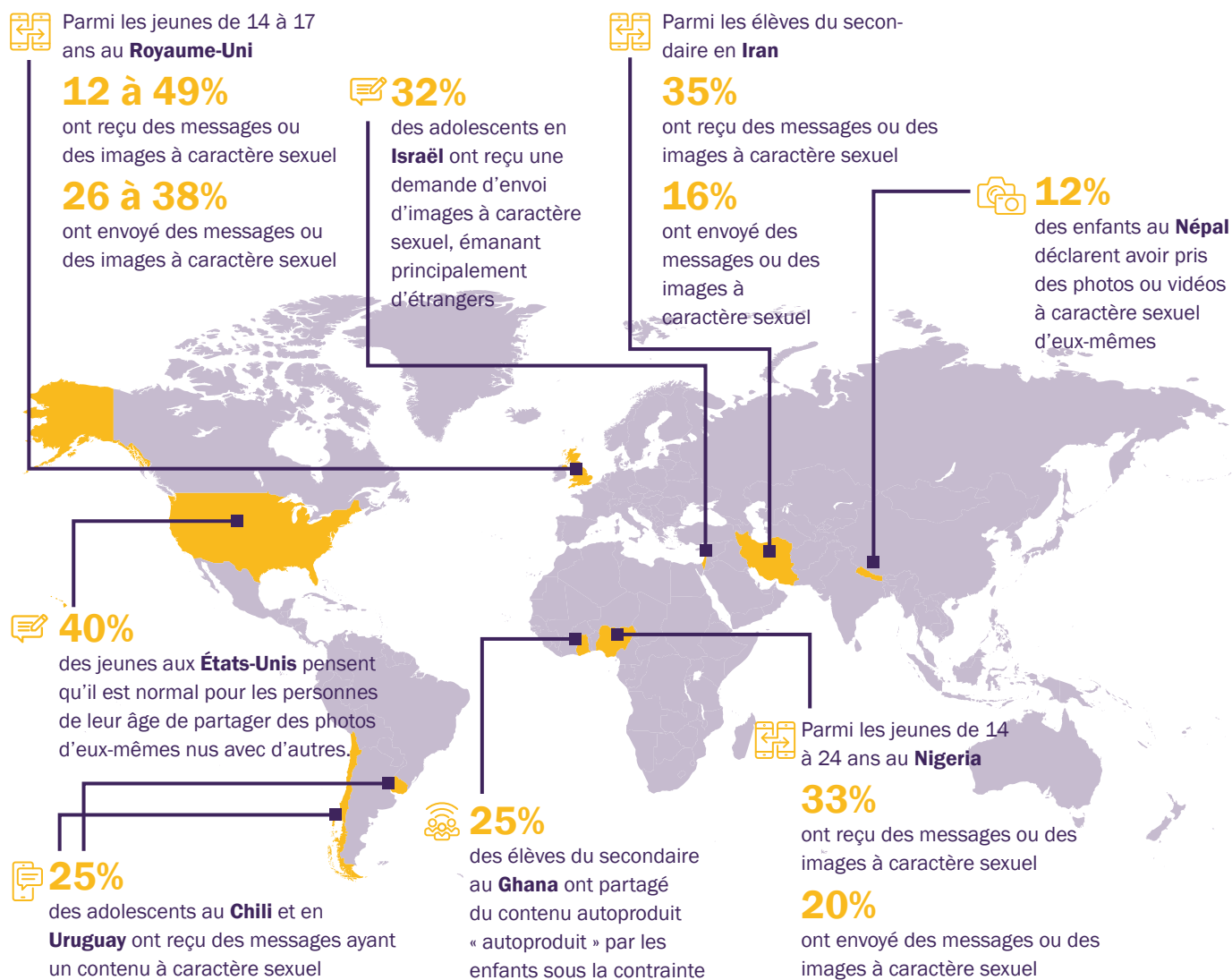
**Dans certains pays, des modifications de la législation permettraient une riposte plus ciblée sur les enfants et plus efficace face à l'émission de matériels d'abus sexuels d'enfants volontairement « autoproduit ».**

Certains cadres juridiques nécessitent une réforme urgente pour éviter le maintien de la criminalisation des enfants pour des comportements qui font sans doute « partie de la découverte normale de la sexualité »<sup>331</sup>.

Dans cette optique, certaines parties de l'Australie ont décriminalisé l'envoi de sextos entre pairs<sup>332</sup>. Ces approches sont possibles selon la Convention de Lanzarote, qui prévoit une exemption de la criminalisation des abus sexuels entre enfants, si certains critères sont remplis. Cette orientation peut aider les nations à déterminer une réponse appropriée à l'égard des enfants et des adolescents impliqués dans la production, la visualisation ou le partage de contenus « autoproduits »<sup>333</sup>. Au Royaume-Uni, le nombre de jeunes qui entrent dans le système pénal pour du contenu à caractère sexuel « autoproduit » a doublé entre 2007 et 2016<sup>334</sup>. Le gouvernement a récemment rappelé aux professionnels de l'éducation que « les enfants et les jeunes qui partagent des images d'eux "nus et semi-nus" ne devraient pas être criminalisés »<sup>335</sup>.

Mais certains jeunes franchissent la ligne rouge des comportements sexuels malveillants et délictueux. Ainsi que l'a souligné l'UNICEF, « les pairs représentent une part significative des coupables d'actes de violence sexuelle commis contre d'autres enfants et adolescents »<sup>336</sup>. Ces scénarios révèlent également une lacune dans la riposte car « les interventions ont été essentiellement conçues pour des délinquants adultes »<sup>337</sup>. La question du contenu à caractère sexuel « autoproduit », qui constitue dans de nombreux cas une agression causée par des pairs, montre l'importance d'établir des stratégies de riposte capables de répondre aux besoins des enfants qui, à la fois, subissent des agressions et s'engagent dans des comportements sexuels préjudiciables envers leurs pairs<sup>338</sup>.

Figure 18: Dans quelle mesure le partage d'images et de messages sexuels est-il répandu chez les jeunes 339 340 341 342 343 344 345 346



# 06 Agressions

## Diffusion en direct d'actes d'exploitation et d'abus sexuels envers les enfants

La diffusion en direct progresse grâce à la connectivité et au faible prix des appareils de streaming.

La diffusion en direct ou live streaming peut porter sur l'agression physique d'un ou de plusieurs enfants, transmise en ligne, ou l'obligation d'exécuter des actes sexuels devant une webcam imposée à un ou des enfants, généralement moyennant paiement.

La diffusion en direct progresse grâce à la connectivité et au faible prix des appareils de streaming. Elle se manifeste souvent sous la forme de crimes transfrontaliers qui nécessitent une riposte internationale coordonnée.

Contrairement à la diffusion en direct autoproduite (voir *Contenu à caractère sexuel « autoproduit » par les enfants* dans le chapitre « Agressions »), ce type d'abus est habituellement facilité par un tiers. Bien que, dans certains cas, les agresseurs et la victime se trouvent dans la même ville, cette forme de criminalité traverse essentiellement les frontières nationales. Comme l'explique l'ECPAT, ce type d'agression a « tendance à tirer parti des disparités économiques, les délinquants de pays développés ayant accès aux victimes dans les pays en développement »<sup>347</sup>. Cette question illustre bien le mal omniprésent dû aux inégalités dans un monde de plus en plus connecté.

Selon Interpol, la diffusion en direct moyennant paiement est en augmentation<sup>348</sup>. Tout porte à croire que la pandémie joue un rôle dans l'accélération de cette tendance. Aux Philippines, un pays décrit par l'UNICEF comme « l'épicentre mondial du commerce d'abus sexuels diffusés en direct »<sup>349</sup>, une augmentation de 265% des cas a été enregistrée pendant le confinement de mars à mai 2020. Save the Children a établi un lien avec l'aggravation de la pauvreté, ce qui suggère que les difficultés économiques créées par la COVID-19 poussent encore davantage de personnes à recourir au live streaming pour de l'argent<sup>350</sup>.

**Cette pratique génère différentes infractions. La plupart des victimes identifiées se trouvent au Sud de la planète, mais des agressions ont lieu dans la plupart des régions du monde.**

Dans les cas de diffusion en direct, les délinquants sont les personnes qui organisent l'exploitation, celles qui mettent en scène le contenu et celles qui le « consomment ». Les personnes qui organisent les agressions peuvent appartenir à des groupes criminels organisés, mais aussi faire partie du cercle de confiance de la victime. Dans son analyse des cas de live streaming aux Philippines, l'IJM a signalé que la majorité des délinquants (69%) étaient des femmes adultes membres de la famille des victimes motivées par une motivation financière ou des proches des victimes<sup>351</sup>. Le fait que les organisateurs de la diffusion en direct de ces images soient principalement motivés financièrement distingue ce crime des nombreuses autres formes d'abus sexuel sur les enfants.

Les données disponibles indiquent que les personnes qui « consomment » ces abus diffusés en direct sont principalement originaires d'Europe, d'Amérique du Nord et d'Australie<sup>352</sup>. Pour rechercher des agressions diffusées en direct, ces délinquants ciblent des régions du monde « présentant des niveaux élevés de pauvreté et possédant des moyens limités de protection à domicile des enfants, avec un accès facile aux enfants »<sup>353</sup>. Les poursuites contre les délinquants « demandeurs » tendent à se concentrer sur le délit de consultation de matériels d'abus sexuels d'enfants, ce qui minimise sans doute leur responsabilité dans la globalité du crime. Comme l'explique l'IJM, il est nécessaire de traiter ces individus comme des trafiquants, parce qu'en rémunérant l'exploitation, ils « abusent de leur pouvoir financier », ce qui correspond à la définition internationalement convenue de la traite d'êtres humains énoncée dans le Protocole de Palerme<sup>354</sup>.

La majorité des victimes de techniques de live streaming ayant été identifiées vivent en Asie du Sud-est, en particulier aux Philippines<sup>355</sup>. Mais il y en a aussi en Europe, en Russie et aux États-Unis<sup>356</sup>. Cela souligne l'importance d'éviter de se limiter à une classification étroite de la diffusion en direct en la caractérisant comme une forme de criminalité ne concernant que les enfants et les jeunes des pays à faible revenu<sup>357</sup>. Selon une étude de cas réalisée en Asie du Sud-Est, non seulement la diffusion en direct d'un tel matériel cause des souffrances et des traumatismes considérables aux victimes, mais elle peut également « constituer pour les enfants une première étape vers une exploitation sexuelle commerciale "hors ligne" »<sup>358</sup>.

## INTERNATIONAL JUSTICE MISSION: l'histoire de Ruby

À 16 ans, Ruby\* a été privée de sa liberté et forcée de faire tout ce que les délinquants en ligne lui demandaient de faire parce qu'ils géraient la diffusion en direct de ses agressions sexuelles.

Le calvaire de Ruby a commencé lorsqu'un trafiquant lui a envoyé un message privé sur un réseau social lui offrant un emploi dans un magasin d'ordinateurs, et a gagné sa confiance en lui disant qu'elle serait nourrie et logée lorsqu'elle travaillerait pour lui. Le trafiquant et sa complice avaient également couvert les frais du voyage de Ruby jusqu'à chez eux. Mais Ruby a vite découvert que le travail n'était pas du tout celui qu'on lui avait promis. Elle a voulu partir, mais s'est trouvée dans l'impossibilité de le faire tant qu'elle n'aurait pas remboursé ce qui était devenu sa « dette » pour rembourser son voyage. Elle a tenté de s'enfuir, mais a été menacée par un couteau.

Ruby décrit les agressions avec ses propres mots:

« J'étais payée pour chaque spectacle dégoûtant que je faisais devant la caméra de l'ordinateur pour le client. Et en faisant chacun de ces spectacles dégoûtants, je perdais un peu de mon estime personnelle au point que je me suis sentie également dégoûtée de moi-même.

C'est comme se trouver enfermé dans une pièce sombre sans aucun rayon de lumière. La vie n'a plus d'intérêt.

Tu fais des spectacles dégoûtants chaque jour, à chaque fois. Puis après avoir fait cela, tu vas dormir et tu recommences la même chose tous les jours. C'est comme s'il n'y avait jamais de fin ».

L'IJM a aidé les autorités philippines à agir sur une information du département américain de la sécurité Homeland Security Investigations (HSI), qui a permis de localiser Ruby et de la sauver, elle ainsi que cinq autres filles. Le couple qui a dirigé l'opération de traite a été arrêté et condamné plus tard, et l'IJM a soutenu Ruby dans son parcours de rétablissement. Voici ce qu'elle a déclaré à propos de ce parcours: « Ce n'était pas du tout facile. Il m'a fallu des années et des années pour me remettre des expériences douloureuses et traumatisantes. Vous savez, la nuit, quand quelqu'un éteint soudainement la lumière, je me lève brusquement de mon lit, je ne peux pas dormir sans lumière allumée parce que j'ai tellement peur de l'obscurité. Voilà dans quel état je me trouve depuis des années ».

Aujourd'hui, Ruby est libre et en sécurité. Elle envisage de suivre une formation juridique dans l'espoir d'aider d'autres filles piégées dans les mêmes conditions.

L'International Justice Mission est une ONG qui collabore avec les systèmes judiciaires locaux du monde entier pour mettre fin à la violence contre les personnes vivant dans la pauvreté. Grâce à son Center to End Online Sexual Exploitation of Children, elle renforce les systèmes visant à protéger les enfants contre la production de matériels d'abus sexuels d'enfants, notamment par le biais de la diffusion en direct.

\* Pseudonyme

### Les frontières de plus en plus floues entre le live streaming et la traite compliquent davantage les enquêtes sur cette technique.

Un tiers des victimes de la traite d'êtres humains détectées dans le monde sont des enfants. Parmi elles, 72% des filles et 23% des garçons sont ciblés à des fins d'exploitation sexuelle<sup>359</sup>. La traite des enfants implique souvent des formes d'agression en ligne et a été associée à la croissance du volume de matériels d'abus sexuels d'enfants disponible. L'Office des Nations Unies contre la drogue et le crime (ONUDC) souligne le cas de trafiquants thaïlandais « exploitant sexuellement un grand nombre d'enfants et produisant plusieurs centaines de milliers d'images pour la distribution en ligne »<sup>360</sup>

. Les limites entre la traite d'êtres humains et la diffusion en direct risquent de devenir de plus en plus floues, car un nombre grandissant de trafiquants font évoluer leurs modèles économiques en ligne pour déjouer l'impact des restrictions dues à la COVID-19<sup>361</sup>. Comme le souligne le Rapport mondial 2021 de l'ONUDC sur la traite des êtres humains, les avantages des technologies Internet pour les trafiquants sont importants, essentiellement: « Elles permettent une exploitation devant un public plus large que ce qui est généralement possible avec la traite traditionnelle »<sup>362</sup>. Tout porte à croire que, du fait de la pandémie, la diffusion en direct a gagné en popularité en tant qu'alternative à la violence sexuelle physique envers les enfants<sup>363</sup>. Les trafiquants en ligne seront sans doute bien placés pour tirer parti de cette augmentation de la demande de services à distance.

Mais lorsque le live streaming a lieu dans le cadre de la traite d'enfants, cela peut créer des difficultés spécifiques qui compliquent les enquêtes. Aux Philippines, l'UNICEF a constaté que les cas de traite liés une exploitation en ligne « étaient confondus avec les affaires de cybercriminalité », un problème susceptible de retarder les signalements<sup>364</sup>. Souvent aussi, les victimes de la traite sont plus difficiles à identifier, précisément du fait du chevauchement avec d'autres formes d'abus<sup>365</sup>.

Un tiers des victimes de la traite  
sont des enfants, dont

**72%** **23%**  
**DE FILLES** **ET** **DE**  
**GARÇONS**

sont ciblés à des fins d'exploitation sexuelle.

## Une collaboration plus proactive est nécessaire entre la police et les prestataires de services en ligne et financiers afin d'améliorer la détection des abus diffusés en direct.

Il est techniquement possible d'interrompre le live streaming. Comme indiqué dans la section *Partage et/ou stockage de matériels d'abus sexuels d'enfants* dans le chapitre « Agressions », des classificateurs existent pour détecter les matériels d'abus sexuels d'enfants. Cependant, la plupart des abus diffusés en direct le sont en ligne dans le cadre de conversations privées et ne sont donc pas soumis à un filtrage ou un examen par un modérateur. Le flux ne laisse habituellement aucune trace, à moins qu'un délinquant ne l'enregistre. Le manque de preuves rend également difficile la poursuite des infractions, un problème aggravé par l'absence de dispositions dans la législation existante pour criminaliser cette pratique<sup>366</sup>. Les consommateurs de pornographie en direct ont en général un faible niveau de sophistication technique (la plupart du live streaming a lieu sur le Web de surface)<sup>367</sup>, sans doute parce qu'ils craignent peu d'être détectés et condamnés.

Certains internautes pourraient considérer comme une intrusion justifiable dans la vie privée la surveillance des conversations privées pour détecter le live streaming. Mais même si de telles procédures étaient acceptées et mises en œuvre par certains prestataires de services en ligne, les délinquants pourraient simplement migrer vers n'importe laquelle des nombreuses plateformes E2EE. Cette fonction masque le contenu des communications, rendant impossible la découverte des flux, ce qui souligne la nécessité urgente de diversifier les méthodes permettant de les interrompre.

Les indicateurs financiers sont cités par beaucoup comme les indices les plus efficaces pour permettre d'identifier les agressions diffusées en direct. De plus, il y a également un précédent de collaboration réussie avec le secteur financier. En 2017, une initiative ciblée aux États-Unis a permis la quasi-élimination de l'utilisation des cartes de crédit pour l'achat de contenu d'abus sexuels d'enfants<sup>368</sup>. L'Australian Transaction Reports and Analysis Center a également réussi à tirer parti de son partenariat public-privé avec la Fintel Alliance pour bloquer les transactions liées à l'exploitation des enfants<sup>369</sup>.

. De nombreux services de police et prestataires de services financiers sont déjà en contact pour enquêter sur les infractions de live streaming. Pourtant, une approche plus proactive serait possible. Comme l'explique l'IJM, les entreprises « s'exécutent normalement » lorsque les forces de l'ordre leur demandent des informations, mais il serait plus important « qu'elles identifient, signalent et interrompent de manière proactive... les transferts d'argent en temps réel »<sup>370</sup>. Le potentiel d'une telle collaboration rapprochée peut être compliqué par la diversification permanente des services financiers. La progression de l'utilisation des cryptomonnaies pourrait également créer des difficultés car, bien qu'il soit possible de tracer ces paiements, les services de police n'ont pas tous le savoir-faire requis<sup>371</sup>.

En 2020, le Groupe Egmont (un consortium de cellules de renseignement financier internationales) a mené une étude sur les utilisations possibles du renseignement financier pour lutter contre le live streaming. Cette étude a mis en évidence certaines difficultés: par exemple, celle qu'il peut y avoir pour faire la différence entre les transactions sur du live streaming et les paiements liés à du contenu pornographique adulte, des escroqueries ou d'autres délits. Dans l'ensemble, la conclusion était qu'il y avait un avantage à « combiner le renseignement financier » avec d'autres sources par un échange de données entre les forces de l'ordre et les entités du secteur privé<sup>372</sup>. Les résultats du projet montrent l'importance d'une approche multisectorielle coordonnée pour lutter efficacement contre les agressions diffusées en direct. Avec des cadres appropriés pour permettre un partage des données en toute légalité, les informations des prestataires de services en ligne pourraient offrir un complément puissant au renseignement financier. Cela pourrait être, par exemple, des signaux (métadonnées et indicateurs comportementaux) indiquant une activité malveillante probable de la part d'utilisateurs.

Une prévention durable du live streaming exige une éducation et une responsabilisation de la communauté, le renforcement des capacités policières et une plus grande cohérence dans l'approche globale.

Une analyse de l'UNICEF sur les cas d'agressions sexuelles en ligne sur des enfants aux Philippines montre que la diffusion en direct est, dans de nombreux cas, facilitée par la famille ou la communauté de la victime et justifiée par certaines croyances culturelles ; par exemple, l'idée qu'il n'y a pas d'agression si l'enfant n'est pas touché ou celle selon laquelle les enfants devraient aider financièrement leur famille<sup>373</sup>. Ce contexte complique la protection (car les enfants dans de telles circonstances peuvent même ne pas reconnaître les agressions) et impose une charge plus lourde aux organismes de protection de l'enfance chargés d'identifier les enfants en danger. L'éducation et la responsabilisation des communautés sont essentielles pour éliminer les croyances préjudiciables et promouvoir des pratiques de protection, afin d'accroître la prise de conscience des dommages causés par ces agressions et prévenir durablement leurs diffusions en direct. Les initiatives qui donnent une voix aux enfants sont également essentielles pour assurer qu'ils soient capables de parler et de demander de l'aide.

Actuellement, il n'existe pas de définition internationalement reconnue du délit d'exploitation et d'abus sexuels envers les enfants par diffusion en direct. Bien que dans de nombreux pays, cela relèverait des dispositions existantes concernant l'exploitation sexuelle des enfants<sup>374</sup>, cette lacune crée un obstacle à la collaboration mondiale des forces de l'ordre et limite la capacité à développer des approches d'enquête cohérentes. Cela signifie également que les délinquants peuvent échapper à la peine prévue par la clause de « double incrimination », qui stipule que le comportement doit être sanctionné à la fois dans le pays d'origine du délinquant et dans celui où l'infraction a eu lieu<sup>375</sup>.

Dans certains pays, les restrictions en matière d'enquêtes réduisent également le risque de détection et de condamnation. En Australie, par exemple, 90% des poursuites pour diffusion en direct qui aboutissent reposent sur l'utilisation de tactiques secrètes. En revanche, au Cambodge, les enquêtes secrètes ne sont pas autorisées par la loi<sup>376</sup>. Au Mexique, les efforts pour lutter contre ces crimes sont entravés par le manque de connaissances des législateurs sur le sujet, qui empêche une considération exhaustive des méthodes de détection et d'enquête<sup>377</sup>.

**Actuellement, il n'existe pas de définition internationalement reconnue du délit de diffusion en direct d'actes d'exploitation et d'abus sexuels envers les enfants.**

# Recommandations

L'évaluation mondiale de la menace montre que l'ampleur de l'exploitation et des abus sexuels en ligne envers les enfants continue à augmenter.

Les recommandations ci-dessous permettraient aux gouvernements, à la société civile, aux communautés et aux prestataires de services en ligne de tirer parti des développements positifs pour améliorer la riposte à la menace, notamment la prévention. Ces recommandations sont adaptées au cadre de travail de la Réponse stratégique mondiale de WeProtect Global Alliance<sup>378</sup>.

L'exploitation et les abus sexuels en ligne envers les enfants constituent un problème mondial, qui exige une collaboration internationale continue et un dialogue intersectoriel. L'Alliance répond à ce besoin en facilitant les échanges entre les gouvernements, le secteur privé et la société civile, et en générant un engagement politique et des approches pratiques pour assurer la sécurité du monde numérique pour les enfants.

**Pour en savoir plus, consultez:** [www.weprotect.org](http://www.weprotect.org)

Thème	Recommandation
Financement	<b>Les gouvernements, le secteur privé et la société civile</b> doivent engager des fonds suffisants pour faire face à la menace de l'exploitation et des abus sexuels en ligne envers les enfants. Les niveaux actuels d'investissement ne sont ni proportionnels à l'ampleur et la portée du problème, ni suffisants pour apporter les changements nécessaires à la riposte mondiale à la menace <sup>379</sup> .
Politique/législation	<p><b>Les gouvernements</b> doivent établir des lois qui criminalisent toutes les infractions liées à l'exploitation et aux abus sexuels en ligne envers les enfants, sur la base de cadres internationaux approuvés, tout en cherchant à éviter la criminalisation des enfants eux-mêmes.</p> <p><b>Les gouvernements</b> doivent investir dans le renforcement des systèmes de protection de l'enfance afin de prévenir l'exploitation et les abus sexuels envers les enfants dans toutes les situations et de riposter à cette menace.</p> <p><b>Les gouvernements</b> doivent envisager des options législatives pour renforcer la réponse à l'exploitation et aux abus sexuels en ligne envers les enfants. Les lois devraient établir des normes concernant les signalements par les secteurs concernés, la suppression rapide du matériels d'abus sexuels d'enfants et une base pour l'utilisation légale et transparente d'outils de détection de ce matériel. Un alignement international devrait être l'objectif à atteindre afin de renforcer la collaboration mondiale pour lutter contre la menace.</p>



<p><b>Justice pénale</b></p>	<p><b>Les gouvernements</b> doivent investir dans la dissuasion et la rééducation afin d'aider les délinquants et ceux qui risquent de le devenir à gérer ou changer leurs comportements.</p> <p><b>Les gouvernements</b> doivent financer des unités de répression spécialisées afin de cultiver et maintenir une expertise en matière de menaces et d'améliorer ainsi les résultats des enquêtes dans les pays. Ils doivent aussi investir dans le renforcement des capacités policières internationales afin de renforcer la collaboration sur la criminalité transfrontalière et technologiquement sophistiquée.</p> <p><b>Les gouvernements</b> et les forces de l'ordre doivent consulter leurs homologues internationaux pour élaborer des approches cohérentes vis-à-vis des enquêtes sur les infractions transfrontalières et résoudre les problèmes courants causés par celles-ci (par exemple, le recueil de preuves dispersées dans plusieurs pays).</p>
<p><b>Services de soutien aux victimes et responsabilisation</b></p>	<p>Afin de réduire le traumatisme lié à la victimisation répétée, les <b>responsables politiques</b> doivent travailler avec <b>le secteur</b> pour établir des normes sur la suppression du matériels d'abus sexuels d'enfants en temps opportun sur Internet ; sur la réduction de la circulation répétée des images ; et sur la conception de formes de signalement adaptées aux enfants et indépendantes des processus de justice pénale.</p> <p><b>Les gouvernements</b> doivent investir dans les services de soutien aux victimes et le renforcement des capacités des services de protection de l'enfance pour s'assurer de disposer d'un personnel formé aux approches vis-à-vis des traumatismes subis et à la façon de soutenir les victimes d'agressions en ligne et d'adapter l'accompagnement des enfants issus de groupes marginalisés.</p> <p><b>Tous les acteurs</b> doivent envisager un engagement sûr et approprié auprès des enfants ayant survécu aux abus sexuels afin d'éclairer la conception de services, de politiques et d'un accompagnement efficaces et de les évaluer.</p>
<p><b>Technologie</b></p>	<p><b>Les prestataires de services en ligne</b> doivent adopter une approche d'intégration de la sécurité à la conception, qui inclut l'évaluation de l'impact de tous les produits et services du point de vue des droits de l'enfant. Ils doivent identifier et, le cas échéant, avertir, expulser et signaler les acteurs qui présentent un risque pour les enfants.</p> <p><b>Les prestataires de services en ligne</b> devraient publier régulièrement des rapports de transparence détaillant les mesures qu'ils prennent pour réduire le risque encouru par les enfants en ligne, ainsi que les mécanismes utilisés pour surveiller leur efficacité.</p> <p><b>Les développeurs de technologies de sécurité en ligne</b> devraient continuer à travailler à l'amélioration de la précision des outils d'estimation de l'âge, des classificateurs permettant de détecter le matériels d'abus sexuels d'enfants inconnu (y compris le contenu diffusé en direct), et des solutions visant à déceler les abus sexuels en ligne sur les enfants dans les environnements chiffrés. L'open sourcing (avec des contrôles appropriés en place) devrait être utilisé pour encourager la collaboration entre les acteurs concernés et contribuer à l'établissement de normes cohérentes pour les technologies de sécurité.</p>
<p><b>Sociétal</b></p>	<p><b>Les gouvernements</b> doivent intégrer la sécurité en ligne aux programmes scolaires en complément de programmes plus larges qui couvrent également les comportements sexuels sains et malveillants, par exemple.</p> <p><b>Toutes les parties prenantes impliquées dans la riposte</b> – y compris les parents, les soignants et les organisations de la société civile – doivent éduquer les communautés sur le risque et l'impact de la violence sexuelle envers les enfants, et sur ce qui peut être fait pour l'empêcher.</p>
<p><b>Recherche et vision</b></p>	<p><b>Les gouvernements, les organisations de la société civile et les prestataires de services en ligne</b> doivent investir dans la recherche pour:</p> <ul style="list-style-type: none"> <li>• Mieux comprendre les voies menant à la délinquance et, dans ce contexte, l'efficacité des programmes de dissuasion, d'auto-assistance et de gestion des délinquants.</li> <li>• Mieux comprendre les facteurs qui sous-tendent l'augmentation du contenu à caractère sexuel « autoproduit » par les enfants, et les caractéristiques du développement social et sexuel des adolescents.</li> <li>• Comprendre les facteurs de risque et de protection qui peuvent augmenter ou réduire le risque de faire d'un enfant une victime, y compris les facteurs spécifiques aux groupes marginalisés.</li> <li>• Mieux comprendre dans quelle mesure les enfants partout dans le monde font l'objet d'une exploitation et d'abus sexuels facilités par la technologie.</li> <li>• Montrer comment se manifeste la menace dans les pays du Sud (car le panorama des preuves dont nous disposons actuellement est plus développé pour les pays du Nord).</li> </ul>

# Remerciements

WeProtect Global Alliance souhaite remercier les personnes et organismes suivants pour leurs conseils dans l'élaboration de l'évaluation mondiale de la menace 2021.

## COMITÉ DIRECTEUR

**Signy Arnason**

Centre canadien de protection de l'enfance

**Rinchen Chopel**

South Asia Initiative to End Violence Against Children

**Sean Coughlan**

Human Dignity Foundation

**Toby Dagg**

INHOPE/Office of the e-Safety Commissioner

**Deborah Denis et Donald Findlater**

Lucy Faithfull Foundation

**Edward Dixon**

Rigr AI

**Nicole Epps**

World Childhood Foundation

**Alexandra Evans**

TikTok

**Guillermo Galarza**

International Centre for Missing and Exploited Children

**Alexandra Gelber**

Ministère américain de la Justice

**Susie Hargreaves**

Internet Watch Foundation

**Afroz Kaviani Johnson**

UNICEF

**Almudena Lara**

Google

**Daniela Ligiero**

Together for Girls

**Remy Malan**

Roblox

**David Miles**

Facebook

**Uri Sadeh**

Interpol

**Michael C. Seto**

University of Ottawa Institute of Mental Health Research at the Royal

**John Starr et Melissa Stroebel**

Thorn

**Nena Thundu**

Union africaine

*Un merci particulier aux membres du Conseil WeProtect Global Alliance et à Getty Images.*



## AUTRES CONTRIBUTEURS/CONTRIBUTRICES

Apple	Unis)
Arpan	National Crime Agency (Royaume-Uni)
Australian Centre to Counter Child Exploitation	Netsweeper
Ministère des Affaires intérieures australien	Palantir
Police fédérale australienne	Policing Institute for the Eastern Region (Royaume-Uni)
Camera Forensics	Project VIC International
ChildSafeNet	SafeToNet
Child Rescue Coalition	SafeBAE
Crisp	Scotiabank
DLT Risk Ltd.	Sentropy
Ethel Quayle	Stuart Allardyce
Europol	Suojellaan Lapsia Ry
Global Partnership to End Violence Against Children (End Violence Partnership)	Terre des Hommes
Dr. Hany Farid	The Technology Coalition
Hamogelo	Ministère de l'Intérieur britannique
International Justice Mission	Ministère britannique du Numérique, de la culture, des médias et des sports
LOCATE	Videntifier
Marie Collins Foundation	Walk Free
Microsoft	YOTI
National Centre for Missing and Exploited Children (États-	ZiuZ Forensic BV

Les conseils apportés dans le cadre de l'élaboration de ce rapport, en tant que membre du comité de direction ou contributeur/ contributrice, ne constituent pas nécessairement un aval (partiel ou total) de son contenu. Les recherches effectuées en vue de l'élaboration et de la rédaction de ce rapport ont été menées par Chloe Setter, Natalia Greene, Nick Newman et Jack Perry.

# Glossaire

Terme	Définition
<b>Abus sexuel sur enfant</b>	Participation d'un enfant à une activité sexuelle qu'il n'est pas pleinement en mesure de comprendre, à laquelle il ne peut consentir en connaissance de cause ou pour laquelle il n'est pas préparé du point de vue de son développement <sup>380</sup> . Il s'agit de la définition de la violence sexuelle envers les enfants adoptée par WeProtect Global Alliance (« l'Alliance »), sur la base des lignes directrices de l'Organisation mondiale de la santé (OMS).
<b>Exploitation sexuelle des enfants</b>	Forme d'abus sexuel sur enfant qui implique l'utilisation abusive ou la tentative d'utilisation abusive d'une position de vulnérabilité, de force ou de confiance. Cela comprend, sans s'y limiter, les avantages monétaires, sociaux ou politiques tirés de l'exploitation sexuelle d'une autre personne <sup>381</sup> . Cette infraction peut être perpétrée par des individus ou des groupes de délinquants. Ce qui distingue l'exploitation sexuelle des enfants des abus sexuels sur enfants est la notion sous-jacente d'échange présente dans l'exploitation <sup>382</sup> . Les deux concepts se chevauchent fortement, car l'exploitation est souvent une caractéristique de l'abus et vice versa <sup>383</sup> .
<b>Exploitation et abus sexuels en ligne envers les enfants</b>	Exploitation et abus sexuels envers les enfants partiellement ou entièrement facilités par la technologie, c'est-à-dire par Internet ou d'autres modes de communications sans fil.  Ce concept est également désigné par l'abréviation anglaise OCSEA (Online Child Sexual Exploitation and Abuse) et ces agressions sont dites « facilitées par la technologie ».
<b>Matériels d'abus sexuels d'enfants</b>	Tout contenu visuel ou audio de nature sexuelle impliquant une personne de moins de 18 ans <sup>384</sup> , réelle ou non.  <b>Remarque sur la terminologie également employée:</b>  certaines organisations font la distinction entre le matériel lié aux abus sexuels sur les enfants et le matériel lié à l'exploitation sexuelle des enfants. (Par exemple, l'Interagency Working Group on the Sexual Exploitation of Children définit le « matériel lié à l'exploitation sexuelle des enfants » comme une catégorie plus large qui englobe le « matériel représentant à la fois des abus et d'autres contenus sexualisés sur les enfants »).  « Pornographie juvénile » est une autre expression également utilisée par certaines organisations. La position affirmée de l'Alliance est de s'abstenir de l'utiliser: « matériels d'abus sexuels d'enfants » est perçu comme une expression qui prend plus précisément en compte la nature odieuse de la violence sexuelle contre les enfants et protège la dignité des victimes.  Certains contenus « autoproduits » par les enfants peuvent également constituer du matériels d'abus sexuels d'enfants, selon les conditions de leur production (voir Matériels d'abus sexuels d'enfants « autoproduit »).



Terme	Définition
<b>Matériels d'abus sexuels d'enfants connu</b>	Matériels d'abus sexuels d'enfants ayant déjà été détecté et classé par les services de répression et/ou les modérateurs.
<b>Matériels d'abus sexuels d'enfants de « première génération »</b>	Matériels d'abus sexuels d'enfants n'ayant jamais été détecté et classé par les services de répression et/ou les modérateurs.
<b>Matériels d'abus sexuels d'enfants non photographique</b>	Il s'agit notamment des caricatures ou dessins générés par ordinateur qui représentent graphiquement des enfants d'une manière sexuellement abusive <sup>385 386</sup> .
<b>Matériel sexualisé d'enfants</b>	<p>Matériel ne mettant pas en scène des abus sexuels sur enfant, mais utilisé à des fins sexuelles. À titre d'exemple, citons une vidéo d'enfants faisant de la gymnastique, consultée de manière inappropriée pour la satisfaction sexuelle.</p> <p>La sexualisation n'est pas toujours un critère objectif et l'élément crucial pour juger une telle situation est l'intention de la personne de sexualiser un enfant dans une image ou de faire usage d'une image à des fins sexuelles.</p>
<b>Production de matériels d'abus sexuels d'enfants</b>	Création de contenu représentant des abus sexuels sur enfants via des photos/ vidéos/enregistrements audio en personne ; création de contenu textuel ou de matériel visuel non photographique (par exemple, généré par ordinateur) ; ou manipulation de matériels d'abus sexuels d'enfants existant pour créer de nouvelles images inédites.
<b>Recherche et/ou consultation de matériels d'abus sexuels d'enfants</b>	Recherche, consultation ou tentative de consultation de matériels d'abus sexuels d'enfants sur Internet.
<b>Partage et/ou stockage de matériels d'abus sexuels d'enfants</b>	Téléchargement, stockage, hébergement et/ou partage de matériels d'abus sexuels d'enfants.

Terme	Définition
<b>Sollicitation d'enfants en ligne à des fins d'exploitation et d'abus sexuels</b>	<p>Établissement par un individu d'une relation, d'un sentiment de confiance et d'un lien émotionnel avec un enfant ou un jeune pour le manipuler, l'exploiter et abuser de lui (ceci étant facilité, partiellement ou entièrement, par Internet ou d'autres modes de communications sans fil)<sup>388</sup>. Il n'y a pas toujours une volonté de rencontre en personne.</p> <p>Remarque sur l'autre terminologie employée: certaines organisations utilisent le terme d'« incitation en ligne » (tel que défini par le NCMEC<sup>389</sup>) pour faire référence à ce concept.</p>
<b>Contenu à caractère sexuel « autoproduit » par les enfants</b>	<p>Contenu de nature sexuelle, notamment les images et vidéos produites par les enfants eux-mêmes, qui les représentent nus ou partiellement nus. Le contenu à caractère sexuel « autoproduit » par les enfants n'est pas une agression en soi (il peut être créé volontairement et partagé dans le cadre d'un échange approprié sur le plan du développement personnel, par exemple, entre adolescents). Toutefois, il existe des scénarios dans lesquels il y a bien une agression qui est commise, notamment:</p> <ul style="list-style-type: none"> <li>• Lorsqu'un enfant ou un adolescent est contraint de créer du contenu à caractère sexuel « autoproduit ».</li> <li>• Lorsque du contenu à caractère sexuel volontairement « autoproduit » est partagé contre la volonté de l'adolescent.</li> </ul> <p>Le présent rapport examine les caractéristiques de l'« auto-production » qui constitue une agression. Ce terme figure entre guillemets tout au long du rapport afin d'éviter de présupposer la volonté de l'enfant ou du jeune concerné. Bien que le contenu produit puisse correspondre à la définition du matériels d'abus sexuels d'enfants, l'intention peut être floue et ne peut en aucun cas être considérée comme acquise.</p>
<b>Diffusion en direct d'actes d'exploitation et d'abus sexuels envers des enfants</b>	<p>Retransmission, en temps réel sur Internet, d'actes d'exploitation ou d'abus sexuels envers des enfants.</p>
<b>Imagerie générée par ordinateur (CGI)</b>	<p>Dans le contexte de l'exploitation et des abus sexuels envers les enfants, ce terme désigne des images sexualisées créées en totalité ou en partie de façon artificielle ou numérique<sup>390</sup>.</p>
<b>« Deepfake »</b>	<p>Forme d'imagerie générée par ordinateur (CGI) qui utilise l'intelligence artificielle pour remplacer l'image d'une personne par une autre dans des photos ou des vidéos enregistrées<sup>391</sup>.</p>
<b>« Capping »</b>	<p>Forme de délinquance qui consiste à capturer des images d'exploitation et d'abus sexuels envers les enfants diffusées en direct<sup>392</sup>.</p> <p>Le capping peut également inclure la capture d'images inoffensives d'enfants et leur utilisation à des fins sexuelles (ces images constitueraient alors des images sexualisées d'enfants).</p>
<b>« Ludification » des abus</b>	<p>L'application d'éléments de type jeu (par exemple, scores, concours avec d'autres, règles de jeu) pour encourager la participation à un abus ou un acte d'exploitation.</p>

Terme	Définition
<b>Affichage de comportements sexuels préjudiciables par un enfant</b>	Enfant ou jeune de moins de 18 ans exhibant des comportements qui sont inappropriés pour son âge, et peuvent être préjudiciables pour lui ou pour les autres et/ou constituer une agression envers un autre enfant, un jeune ou un adulte <sup>393</sup> .
<b>Facteurs de risque</b>	Facteurs individuels, relationnels, communautaires et sociétaux qui peuvent accroître la probabilité qu'un enfant fasse l'objet d'un acte d'exploitation ou d'abus sexuels.
<b>Facteurs de protection</b>	Facteurs individuels, relationnels, communautaires et sociétaux qui peuvent réduire le risque qu'un enfant fasse l'objet d'un acte d'exploitation ou d'abus sexuels.
<b>Revictimisation</b>	Situation dans laquelle une victime fait face à une agression ou un abus sexuel après une première agression ou un premier abus <sup>394</sup> . Cela inclut les nouveaux transferts et consultations d'images sur Internet: une seule et même image d'une victime peut être partagée des centaines ou des milliers de fois <sup>395</sup> . La revictimisation peut être causée par le même agresseur ou par un agresseur différent de celui à l'origine de la victimisation initiale.
<b>Traite d'enfants</b>	Recrutement, transport, transfert, hébergement ou réception d'enfants à des fins d'exploitation <sup>396</sup> .
<b>Pays du Nord</b>	Les pays du G8, les États-Unis, le Canada, tous les États membres de l'Union européenne, l'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 <sup>397</sup> .
<b>Pays du Sud</b>	L'Afrique, l'Amérique latine, le Moyen-Orient et l'Asie émergente. Ils comprennent trois des quatre nouvelles économies avancées du BRIC (exception faite de la Russie): Brésil, Inde et Chine <sup>398</sup> .
<b>Web de surface</b>	Partie du Web qui est disponible au grand public et sur laquelle des recherches peuvent être effectuées avec des moteurs de recherche de base <sup>399</sup> .
<b>Web profond</b>	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 adresse IP ou un lien direct et cela peut nécessiter un mot de passe ou d'autres mesures de sécurité au-delà de la page Web publique <sup>400</sup> .
<b>Dark Web</b>	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 chiffré et les pages Web sont hébergées de manière anonyme <sup>401</sup> .

Terme	Définition
<b>Technologie de sécurité (Safety Tech)</b>	Solutions destinées à favoriser les expériences en ligne plus sûres et à protéger les utilisateurs contre les contenus, les contacts ou les comportements malveillants <sup>402</sup> .
<b>Sécurité intégrée à la conception</b>	Intégration, dès le départ, des droits et de la sécurité des utilisateurs à la conception et aux fonctionnalités des produits et services en ligne <sup>403</sup> .
<b>Pair-à-pair (P2P)</b>	Dans un réseau P2P, les « pairs » sont des systèmes informatiques connectés les uns aux autres via Internet. Les fichiers peuvent être partagés directement entre les systèmes du réseau sans avoir besoin d'un serveur central. En d'autres termes, chaque ordinateur d'un réseau P2P devient un serveur de fichiers ainsi qu'un client <sup>404</sup> .
<b>Réseau virtuel privé (Virtual Private Network ou VPN)</b>	Processus de création d'une connexion Internet chiffrée entre un appareil et un réseau ; on parle aussi de tunnel <sup>405</sup> .
<b>Hachage</b>	Processus par lequel une valeur de hachage binaire est créée par un algorithme mathématique qui transforme des données de toute taille en données de longueur fixe beaucoup plus courtes. Cette séquence plus courte représente les données d'origine et devient la signature unique du fichier concerné ou sa valeur de hachage, souvent désignée par empreinte numérique <sup>406</sup> .
<b>Correspondance de hachage</b>	Processus qui consiste à utiliser des bases de données de hachage de matériels d'abus sexuels d'enfants pour détecter le moment où ce matériel est repartagé, en faisant correspondre sa valeur de hachage à celle de fichiers déjà connus <sup>407</sup> .
<b>Classification ou modération basée sur l'intelligence artificielle (IA)</b>	Systèmes de modération entièrement ou partiellement automatisés qui identifient le contenu malveillant en suivant des règles et en interprétant de nombreux exemples de contenu malveillant ou non <sup>408</sup> .
<b>Chiffrement</b>	Processus qui consiste à coder l'information sous une autre forme qui ne peut être déchiffrée que par les personnes autorisées qui détiennent la clé de déchiffrement <sup>409</sup> .
<b>Chiffrement de bout en bout</b>	Forme de chiffrement dans laquelle le contenu de chaque message est visible uniquement par l'expéditeur et le destinataire. Le déchiffrement du message nécessite l'échange d'une clé de déchiffrement privée entre les correspondants de sorte que, même si le message est intercepté, il ne peut être ni visualisé ni surveillé par le prestataire de services, les services de répression ou tout autre tiers <sup>410</sup> .
<b>« Services cachés »</b>	Sites Web hébergés dans un réseau proxy (comme Tor) afin d'empêcher leur localisation <sup>411</sup> .
<b>Métadonnées</b>	Données décrivant d'autres données <sup>412</sup> . Parmi les exemples de métadonnées, citons l'heure et la durée d'un appel téléphonique (par opposition au contenu de la communication elle-même).
<b>Tor</b>	Réseau en open source qui garantit la confidentialité en permettant aux utilisateurs de naviguer sur le Web de façon anonyme. Ce système utilise une série de nœuds superposés pour masquer les adresses Web, les données en ligne et l'historique de navigation <sup>413</sup> .



Terme	Définition
<b>Outils sécurisés</b>	Logiciels et applications utilisés pour favoriser l'anonymat en ligne en masquant l'identité et la localisation des utilisateurs.
<b>Systèmes d'exploitation sécurisés</b>	Utilisation de systèmes d'exploitation pouvant être démarrés à partir d'une clé USB. Comme ils n'écrivent pas sur le disque dur, une fois qu'ils sont éteints, tout est supprimé. Un logiciel de chiffrement peut ensuite être utilisé pour protéger le contenu d'un fichier et de parties du disque dur, afin que ce contenu ne soit accessible qu'avec la clé de déchiffrement de l'utilisateur.
<b>Techniques de dissimulation</b>	Ensemble de techniques d'occultation et de stratégies d'évasion en constante évolution, que les délinquants utilisent pour éviter la détection individuelle, ainsi que celle de leurs techniques et stratégies visant à identifier et impliquer des enfants.
<b>Virtualisation et émulation</b>	Les machines virtuelles permettent aux utilisateurs d'exécuter un système d'exploitation qui se comporte comme un ordinateur complet distinct dans une fenêtre d'application sur leur bureau. Certains émulateurs peuvent créer une interface de smartphone virtuel sur un ordinateur. Cela permet à l'utilisateur d'installer et d'utiliser sur son ordinateur des applications qui ne seraient pas disponibles autrement. Les émulateurs sont souvent utilisés en conjonction avec des outils de « capping », car ils peuvent empêcher l'envoi d'une notification de la capture d'écran à la victime, et le délinquant peut utiliser le logiciel de « capping » installé sur son ordinateur pour capturer des images plus nettes.
<b>Convention des Nations Unies relative aux droits de l'enfant</b>	Un traité international sur les droits de l'homme, qui comprend 54 articles couvrant tous les aspects de la vie d'un enfant et définit les droits civils, politiques, économiques, sociaux et culturels auxquels tous les enfants du monde entier ont droit. Il explique également aux adultes et gouvernements comment travailler de concert pour s'assurer que tous les enfants puissent jouir de tous leurs droits <sup>414 415</sup> .
<b>Comité des droits de l'enfant des Nations Unies, Observation générale n° 25</b>	Directives faisant autorité et définissant la manière dont les droits des enfants s'appliquent dans l'environnement numérique. Elles aident les États à comprendre quelles mesures sont nécessaires pour respecter, protéger et respecter les droits des enfants dans l'environnement numérique <sup>416</sup> .
<b>Principes volontaires de lutte contre l'exploitation et les abus sexuels envers les enfants</b>	Ensemble de principes visant à fournir un cadre pour lutter contre l'exploitation et les abus sexuels en ligne envers les enfants et destinés à piloter une action collective. Ils ont été élaborés par cinq gouvernements (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis), en consultation avec de nombreux intervenants, notamment un groupe de représentants éminents du secteur <sup>417</sup> .
<b>Modèle de réponse nationale WeProtect Global Alliance</b>	Cadre fournissant des conseils et un accompagnement aux pays et aux organisations pour les aider à mettre en œuvre le modèle de réponse nationale. Ce modèle vise à aider les pays à développer leur riposte à l'exploitation sexuelle des enfants en ligne <sup>418</sup> .
<b>Réponse stratégique mondiale WeProtect Global Alliance</b>	Cadre fournissant des conseils et un accompagnement aux pays et aux organisations pour les aider à mettre en œuvre la réponse stratégique mondiale. Ce modèle vise à renforcer la collaboration internationale sur la riposte à l'exploitation sexuelle des enfants en ligne.
<b>Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (également connue sous le nom de « Convention de Lanzarote »)</b>	Une convention qui exige la criminalisation de toutes sortes de délits sexuels contre les enfants. Elle prévoit que les États d'Europe et d'ailleurs adopteront une législation spécifique et prendront des mesures pour prévenir la violence sexuelle, protéger les enfants qui en sont victimes et poursuivre les auteurs de ces actes. Le « Comité Lanzarote » est l'organe créé pour surveiller que les parties mettent en œuvre la Convention de Lanzarote de manière efficace et identifier les bonnes pratiques <sup>419</sup> .
<b>Directive européenne relative à la vie privée et aux communications électroniques</b>	Législation concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques <sup>420</sup> . La directive ne contient pas de base juridique explicite permettant de poursuivre les pratiques volontaires actuelles visant à détecter, signaler et éliminer les abus sexuels sur les enfants <sup>421</sup> .

# 10

# Annexe A:

## Résultats de l'enquête de WeProtect Global Alliance/Technology Coalition sur les entreprises technologiques

### CONCLUSIONS SOMMAIRES

Bon nombre des entreprises interrogées ont la capacité de détecter l'exploitation et les abus sexuels en ligne envers les enfants et de mettre en place des mécanismes de signalement. Mais il existe des possibilités d'amélioration sur le plan de la collaboration et du degré de priorité accordée à la dissuasion et la prévention.

	Rapports	Détection	La dissuasion et la prévention	Développement d'outils	Transparence rapporter
Principales conclusions	La plupart des rapports sont au moins en partie automatisés, et presque toutes les entreprises ont une forme de mécanisme de rapport	La majorité des entreprises utilisent des outils basés sur le hachage pour détecter à la fois l'image et la vidéo abus sexuel sur enfant. Utilisation de classificateurs avancés pour détecter la vidéo et le contenu en direct, est moins fréquent malgré le fait que cette catégorie soit devenue plus répandue	Mesures de prévention comme la dissuasion par messagerie et l'enfant les ressources de sécurité sont largement fournies, mais ceux-ci sont moins fréquents que l'utilisation de hash pour la détection, malgré leur potentiel d'empêcher les abus avant qu'ils ne se produisent	De nombreuses entreprises utilisent des outils développés par d'autres, mais c'est moins commun pour eux de développer des outils internes et les partager	La plupart des entreprises ne publient encore de transparence dans leurs rapports. Cependant, de nombreuses entreprises qui le font, ont une grande majorité de données publiées spécifiques sur l'exploitation sexuelle et l'exploitation
Recommandations	Diversifier les voies de reporting pour acquérir une image plus holistique de la menace	Partager des informations et l'intelligence (par exemple, les hachages et les mots-clés) pour aider à rester en avance sur ce qui est un espace en évolution rapide	Investir dans la dissuasion et les mesures de prévention, et diversifier les cibles de la sécurité en ligne pour éviter trop de confiance en un groupe, pour aider à prévenir les abus avant qu'ils ne se produisent	Collaborer et partager des outils dans l'ensemble de l'industrie pour aider à maximiser leur efficacité. Assurer que les cadres réglementaires responsabilisent plutôt que entravent les entreprises à utiliser des outils clés	Développer l'universel des cadres de reporting à s'assurer que les données sont cohérentes et encourager plus les entreprises à le faire. Disponible publiquement

## MÉTHODOLOGIE

En février et mars 2021, WeProtect Global Alliance et la Technology Coalition ont mené une enquête comportant 20 questions auprès de membres de leur secteur respectif afin de comprendre la portée des activités entreprises par les sociétés technologiques pour lutter contre le problème de la violence sexuelle en ligne envers les enfants. Au total, 32 entreprises, avec un effectif de moins de 250 employés à plus de 5 000 employés, ont répondu.



## LIMITATIONS

L'échantillon est très limité par rapport à la taille du secteur mondial de la technologie et il est plus représentatif des entreprises situées dans les pays du Nord. Toutefois, la grande diversité de tailles et de types des entreprises ayant participé à cette enquête donne sans doute un échantillon représentatif de ce secteur. Étant donné que l'enquête a été entièrement anonymisée et agrégée, il n'a pas été possible de retracer les réponses d'un participant donné à plusieurs questions, ce qui a limité les comparaisons possibles entre les réponses, par exemple, selon la taille de l'entreprise. Enfin, certaines des questions pouvaient ne pas concerner tous les participants. Cela a été atténué par l'inclusion d'une option « S/O » ou la possibilité d'ignorer des questions.

# RÉSULTATS COMPLETS

## Signalements:

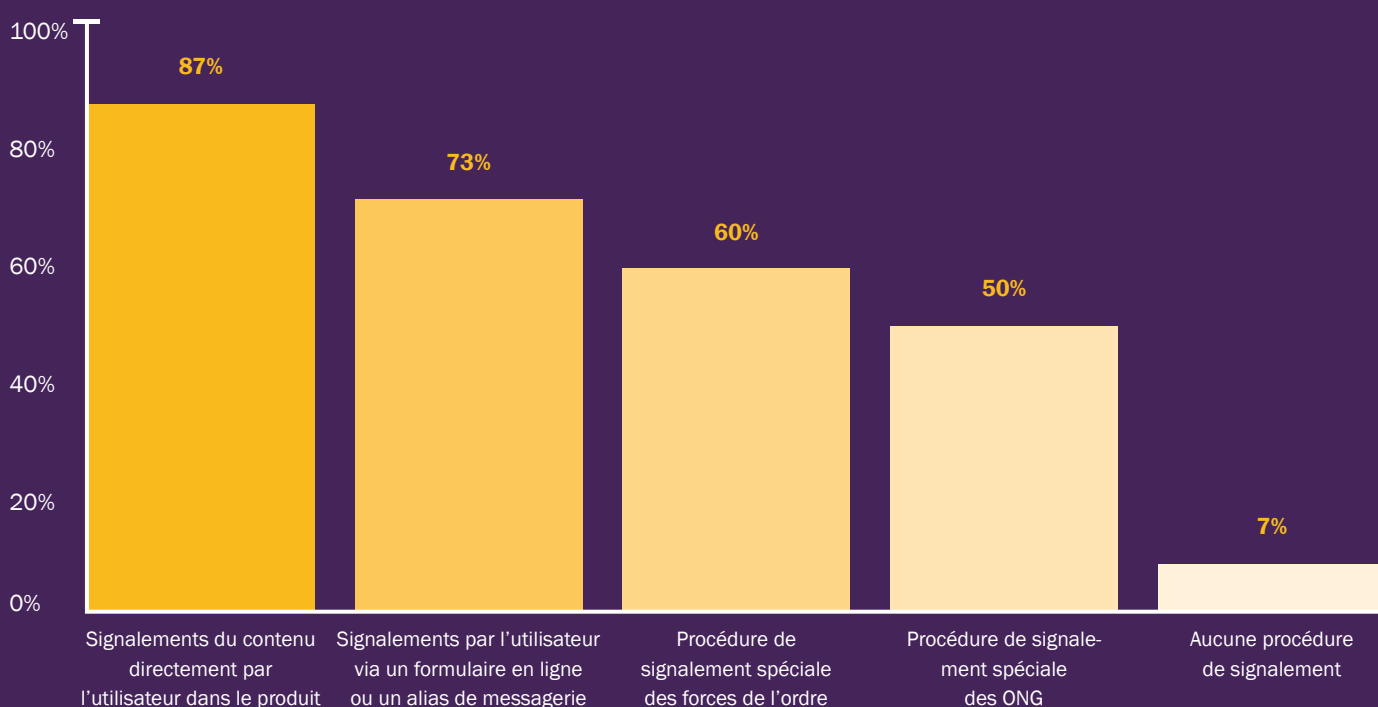
Sur les entreprises interrogées, 84% ont au moins des processus partiellement automatisés pour la transmission des signalements d'abus sexuels en ligne envers les enfants, ce qui laisse entendre que la gestion des signalements est relativement efficace.

Mais cette question ne portait pas sur les mécanismes de détection proactifs que les entreprises peuvent avoir mis en place, et ne fournit donc pas une vue d'ensemble complète à cet égard. Toutefois, en dehors de cela, le mécanisme de signalement le plus répandu dans les entreprises est celui du signalement direct par les utilisateurs. Les moins courants sont les modes de signalement proposés par les ONG et des forces de l'ordre, ce qui laisse entendre qu'il pourrait y avoir une plus grande collaboration intersectorielle. La diversification des modes de signalement permettra également d'éviter une dépendance excessive aux signalements par les utilisateurs, et pourrait contribuer à fournir un panorama plus complet des infractions, étant donné que les taux de signalements volontaires sont peu élevés.



Figure 19: Mécanismes fournis par les sociétés pour les signalements.

### Quels sont les systèmes fournis par les sociétés pour le signalement du matériel d'abus sexuels d'enfants?



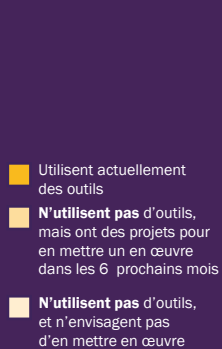
# DÉTECTION

## Détection basée sur le hachage

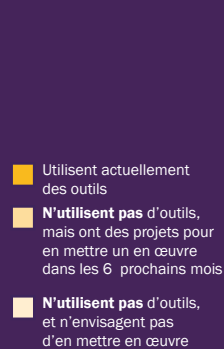
La plupart des participants utilisent des outils basés sur le hachage pour détecter les images et les vidéos d'abus sexuels d'enfants sur leurs plateformes ; et la majorité de ceux qui n'utilisent pas encore ce type d'outils prévoit de les mettre en œuvre au cours des six prochains mois, comme le montre la figure 20 ci-dessous.

Figure 20: Utilisation des outils de détection basés sur le hachage par les sociétés

Quelle est la proportion d'entreprises utilisant des outils de détection basés sur le hachage d'images?



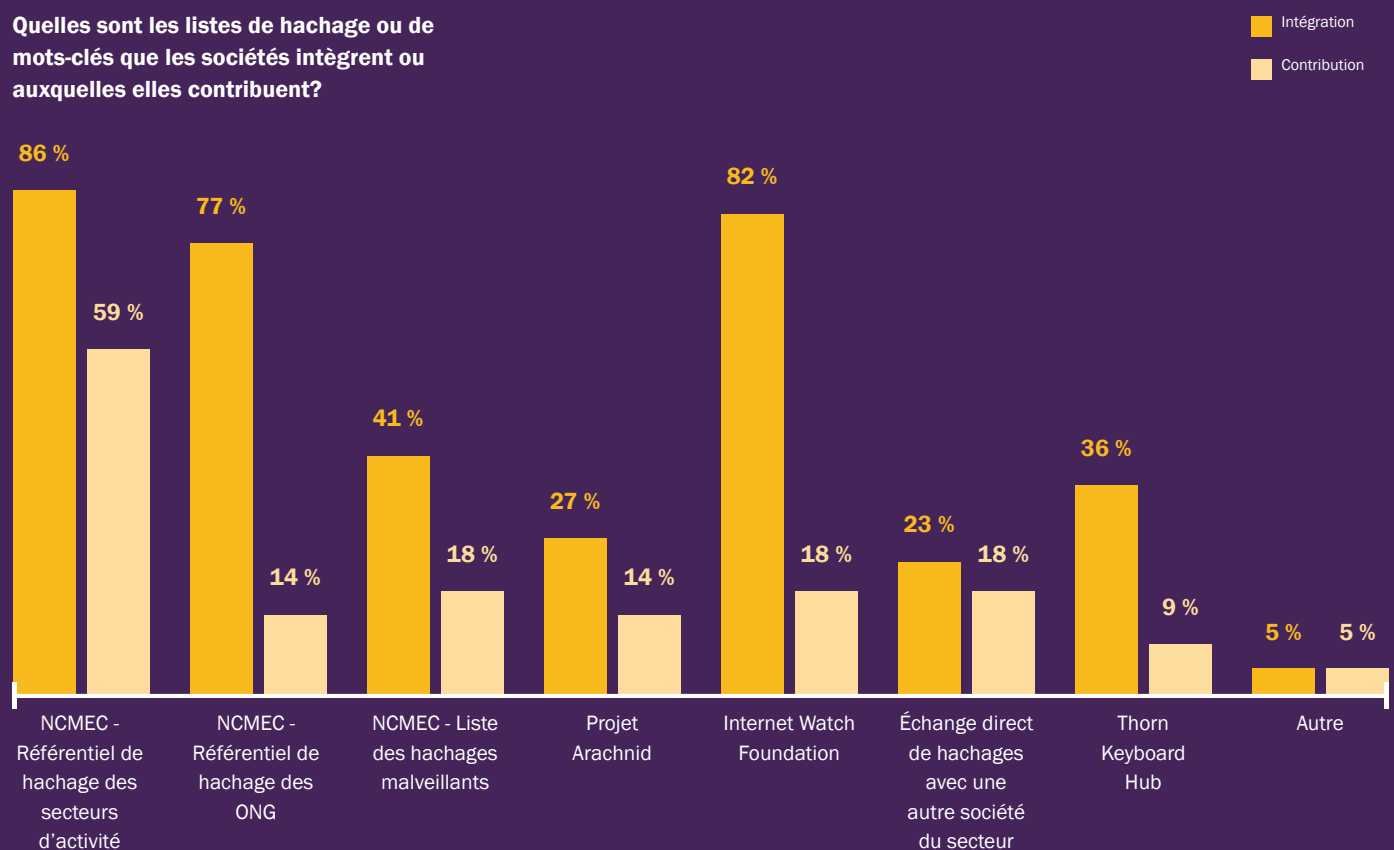
Quelle est la proportion d'entreprises utilisant des outils de détection basés sur le hachage de vidéos?



Pour utiliser efficacement les outils de détection basés sur le hachage, les entreprises doivent avoir accès à des hachages de matériels d'abus sexuels d'enfants connu. Un autre élément important de la détection est la capacité à bloquer les termes de recherche relatifs aux abus sexuels sur les enfants et, pour cela, les entreprises ont besoin d'accéder à des listes de mots-clés.

La plupart des entreprises intègrent les hachages et les mots-clés à partir d’au moins un référentiel, comme illustré à la figure 21 ci-dessous. Cependant, une fraction bien plus faible contribue aux listes de hachages et de mots-clés. En supposant que les entreprises ne détectent pas uniquement le contenu connu, un partage limité de renseignements externes pourrait avoir un impact sur la capacité à suivre l’évolution de la menace.

Figure 21: Utilisation des listes de hachages/mots-clés par les sociétés.

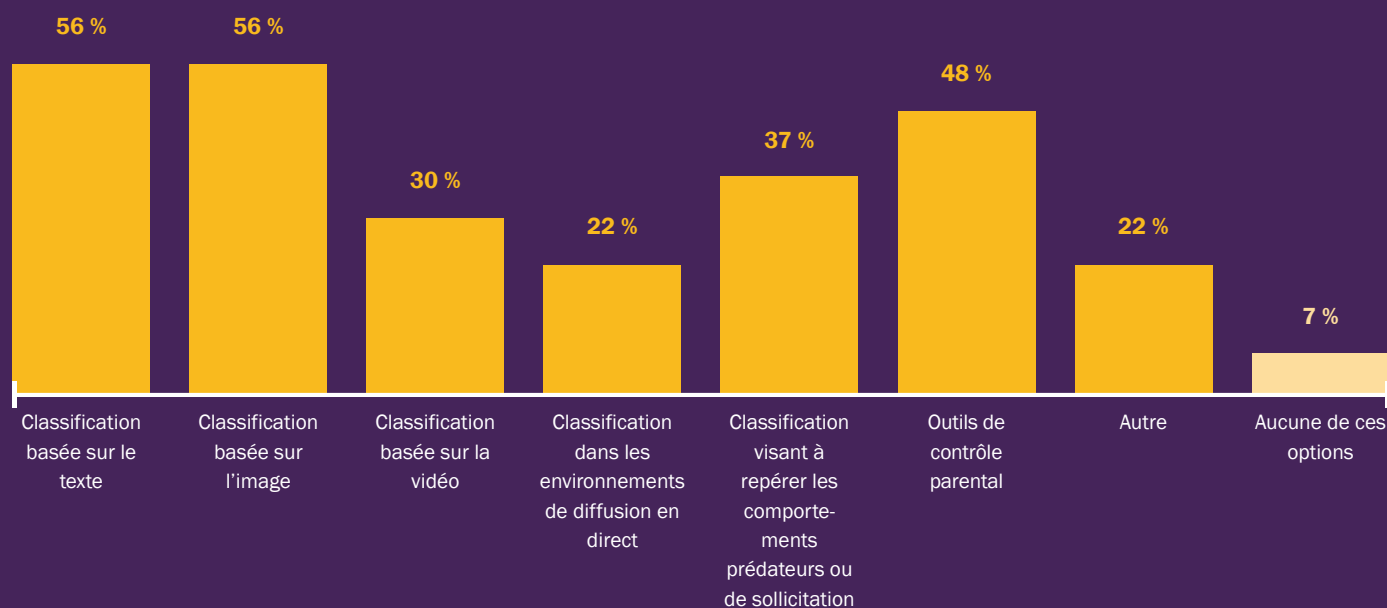


## DÉTECTION AVANCÉE

La détection avancée fait référence à des technologies telles que les classificateurs basés sur l'intelligence artificielle. Ces mesures de détection sophistiquées sont moins répandues que celles basées sur le hachage. Malgré les données indiquant une prévalence croissante du contenu vidéo et diffusé en direct, les classificateurs destinés à détecter ce type de contenu ne sont utilisés que par 30% et 22% des participants respectivement.

Figure 22: Mesures supplémentaires pour lutter contre l'exploitation et les abus sexuels en ligne envers les enfants.

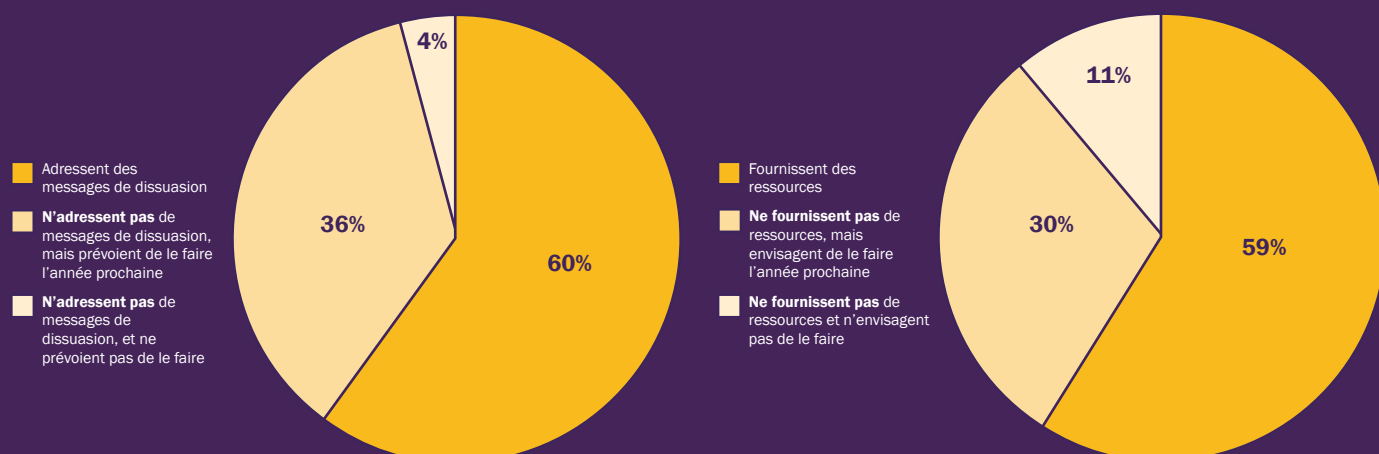
**Quelles sont les mesures complémentaires utilisées par les sociétés pour lutter contre l'exploitation et les abus sexuels en ligne envers les enfants?**



## DISSUASION ET PRÉVENTION

La plupart des participants adressent des messages de dissuasion aux délinquants potentiels et fournissent des ressources pour la protection des enfants en ligne, afin de prévenir les abus. Mais ces deux méthodes sont moins courantes que les mécanismes de détection de matériels d'abus sexuels d'enfants.

Figure 23: Utilisation par les entreprises de messages de dissuasion et de ressources pour la protection des enfants en ligne.



L'enquête montre que la plupart des ressources en ligne destinées à protéger les enfants s'adressent aux parents, ce qui est en soi positif car ils sont le premier point de contact d'un enfant qui éprouve un sentiment de détresse en ligne<sup>422</sup>. Cependant, les faits montrent que l'exploitation et les abus sexuels envers les enfants sont souvent commis par des membres de la famille<sup>423</sup>. Pour soutenir les enfants victimes de ces situations et éviter de s'appuyer excessivement sur un seul groupe pour les protéger, il est possible d'offrir davantage de ressources aux enfants eux-mêmes, aux éducateurs et à d'autres publics.

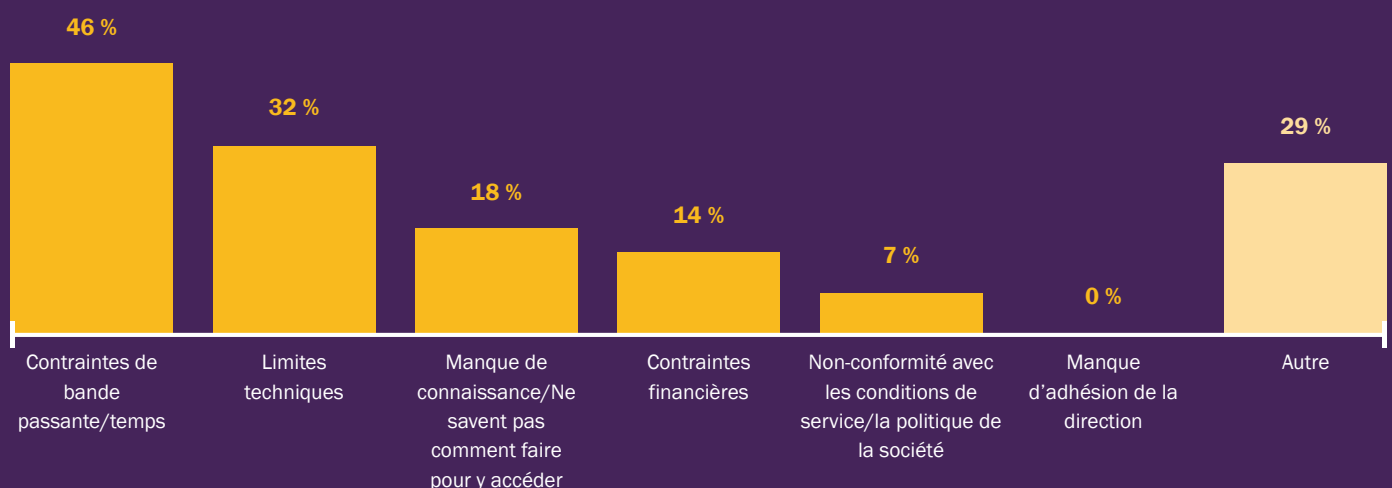


## DÉVELOPPEMENT D'OUTILS

Près de 50% des entreprises interrogées utilisent des classificateurs de contenu développés par d'autres sociétés, mais seulement 26 % rendent accessibles aux autres les outils qu'elles développent elles-mêmes. Une enquête plus approfondie serait nécessaire pour comprendre les raisons de cette situation. Une intensification de la collaboration et du partage des outils, dans la mesure du possible, pourraient probablement contribuer à optimiser globalement les avantages de ces outils.

Figure 24: Obstacles à l'utilisation d'outils pour lutter contre les abus sexuels en ligne sur les enfants.

**Quels sont les obstacles auxquels sont confrontées les entreprises dans l'utilisation des ressources techniques pour lutter contre l'exploitation et les abus sexuels en ligne envers les enfants?**



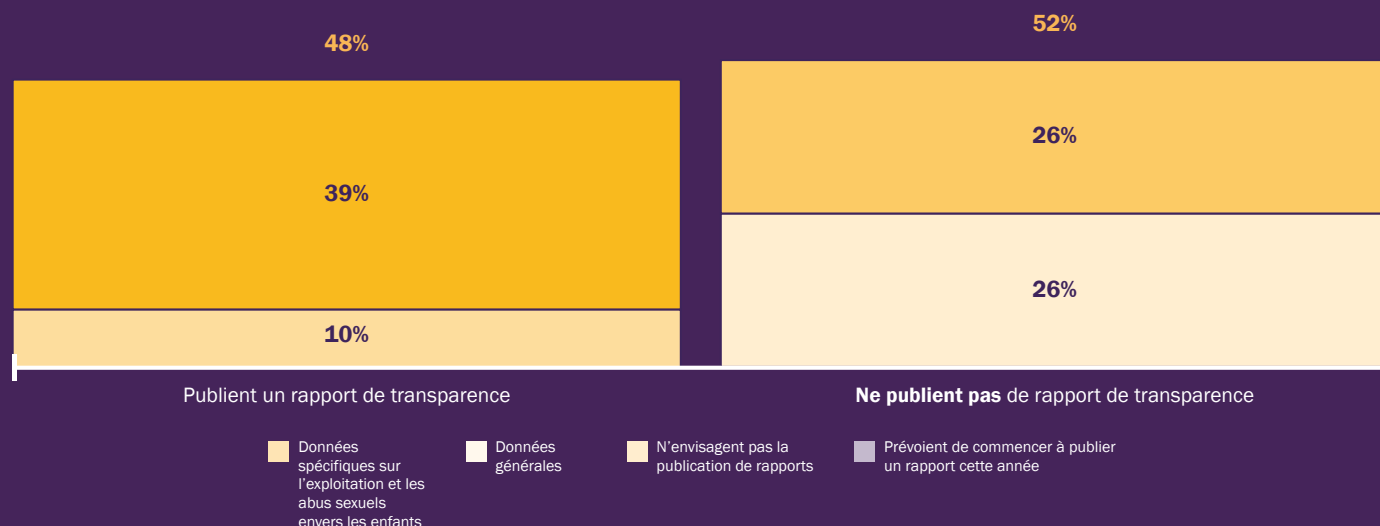
Les contraintes de temps et de bande passante sont les principaux obstacles empêchant les entreprises de développer et déployer des outils pour lutter contre les abus sexuels en ligne sur les enfants. Le manque d'adhésion de la part des dirigeants n'a pas été cité comme un problème par les participants.

# TRANSPARENCE

Une culture de la transparence est essentielle pour permettre une riposte commune et informée à l'exploitation et aux abus sexuels en ligne envers les enfants. Toutefois, seulement 49% des participants publient régulièrement un rapport de transparence. Et sur ce chiffre, 80% publient des données spécifiques sur l'exploitation et les abus sexuels envers les enfants, ce qui est essentiel pour comprendre l'ampleur et la portée de la menace

Figure 25: Rapports de transparence des entreprises

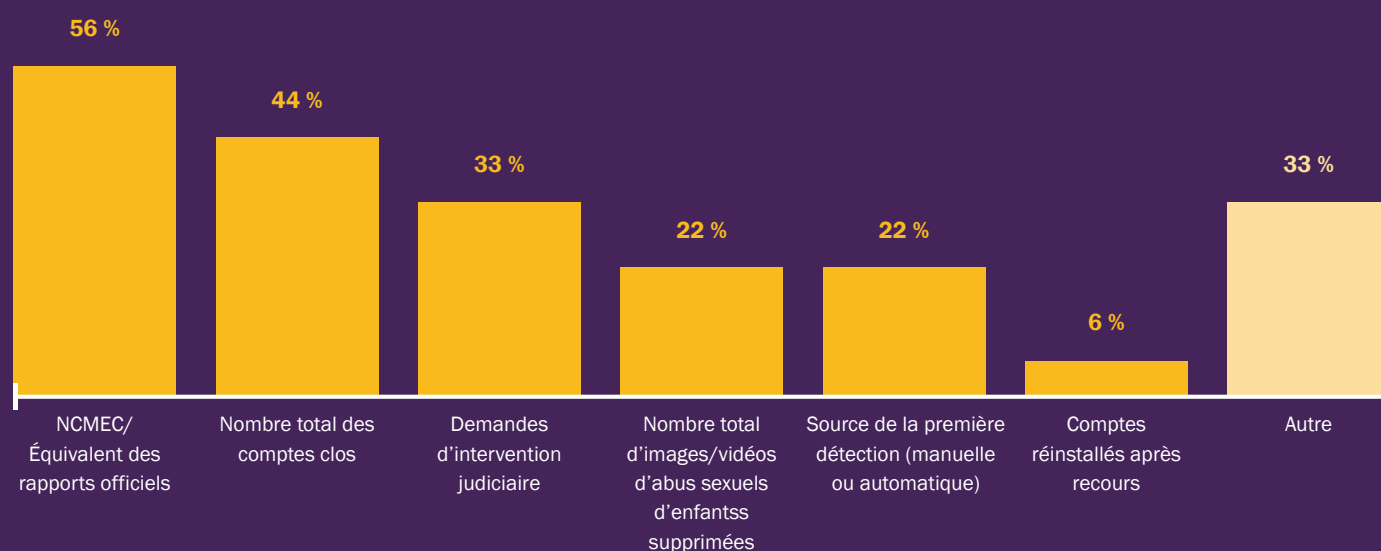
Quelle est la proportion des entreprises qui publient régulièrement des rapports de transparence sur l'exploitation et les abus sexuels sur enfants sur leur plateforme?



Les données rapportées par les entreprises peuvent être très variées, comme le montre la figure 26 ci-dessous. Il faudra des efforts supplémentaires pour développer des cadres universels pour la production de rapports. Cela permettrait d'obtenir des données cohérentes et comparables, et encouragerait les entreprises qui ne publient pas encore leurs données à les rendre publiques.

Figure 26: Types de données figurant dans les rapports de transparence.

**Quel est le type de données relatives à l'exploitation et aux abus sexuels en ligne envers les enfants figurant dans les rapports de transparence émis par les sociétés qui en publient?**



La figure 26 montre qu'il est courant pour les entreprises de présenter des données agrégées, comme le nombre total de contenus d'abus sexuels d'enfants supprimés. Cependant, les données issues des rapports de transparence sont rarement ventilées pour montrer la prévalence des différents types d'abus sexuels sur les enfants, comme les sollicitations ou la diffusion en direct. Un rapport sur ces chiffres offrirait davantage de visibilité sur les lieux où se multiplient les différentes agressions afin de mener des interventions spécifiques ciblées là où elles sont le plus nécessaires.

# References

- 1 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 2 4 arrested in takedown of dark web child abuse platform with some half a million users (Europol, 2021) Accessed from: <https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users> 04/05/2021
- 3 NetClean Report COVID-19 Impact 2020 (NetClean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/#> 04/05/2021
- 4 Fighting Child Exploitation with Big Data (Freethink, 2020) Accessed from: <https://www.freethink.com/videos/child-exploitation> 16/06/2021
- 5 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBAR-GO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021
- 6 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-2/> 26/01/2021
- 7 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: <https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020> 24/02/2021
- 8 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends> 22/04/2021
- 9 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: [https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm\\_source=ActiveCampaign&utm\\_medium=email&utm\\_content=New+briefings+and+reports+from+the+Alliance+and+our+members&utm\\_campaign=May+2021+newsletter](https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+from+the+Alliance+and+our+members&utm_campaign=May+2021+newsletter) 07/06/2021
- 10 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse> 26/01/2021
- 11 By the Numbers (NCMEC, 2021) Accessed from: <https://www.missingkids.org/gethelpnow/cybertipline> 16/06/2021
- 12 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 13 Action to end Child Sexual Abuse and Exploitation (UNICEF, 2020) Accessed from: <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 23/07/2021
- 14 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 15 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden> 22/04
- 16 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021
- 17 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: <https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimmas-en-lo-corrido-de-2021> 11/03/2021
- 18 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: <https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/> 25/02/2021
- 19 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: [https://www.aic.gov.au/sites/default/files/2021-02/ti616\\_production\\_and\\_distribution\\_of\\_child\\_sexual\\_abuse\\_material\\_by\\_parental\\_figures.pdf](https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf) 09/03/2021
- 20 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: <https://protect-eu.mimecast.com/s/WuEPCWn-WgFxBY3Hxchqm?domain=levante-emv.com> 23/02/2021
- 21 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBAR-GO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021

- 22 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf> 17/06/2021
- 23 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 24 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: [https://www.who.int/violence\\_injury\\_prevention/publications/violence/med\\_leg\\_guidelines/en/](https://www.who.int/violence_injury_prevention/publications/violence/med_leg_guidelines/en/) 19/04/2021
- 25 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: [https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines\\_en.pdf](https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf) 25/05/2021
- 26 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: [https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines\\_ENG.pdf](https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf) (23/07/2021)
- 27 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 26/01/2021
- 28 Grooming (NSPCC) Accessed from: <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/> 25/05/2021
- 29 Online Enticement (NCMEC) Accessed from: <https://www.missingkids.org/netsmartz/topics/onlineenticement> 25/05/2021
- 30 Netclean Annual Report; Comment to insight 4 – Simon Bailey (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-6/> 17/06/2021
- 31 Netclean Annual Report; Insight 2: Online Child Sexual Abuse Activity has increased (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-2/> 07/06/2021
- 32 Netclean Annual Report; Comment to insight 4 – Rob Jones (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-6/> 17/06/2021
- 33 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: [https://reliefweb.int/sites/reliefweb.int/files/resources/A\\_HRC\\_46\\_31\\_E.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf) 07/06/2021
- 34 Protection of children should always trump protection of privacy (eSafety Commissioner, 2020) Accessed from: <https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy> 07/06/2021
- 35 Abuso sexual infantil crece en un 50% durante la pandemia por coronavirus (El Imparcial, 2021) Accessed from: <https://www.elimparcial.com/mundo/Abuso-sexual-infantil-crece-en-un-50-durante-la-pandemia-por-coronavirus-20210216-0011.html> 07/06/2021
- 36 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: <https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children> 22/04/2021
- 37 La pornografía infantil creció 117% en México (Jornada, 2020) Accessed from: <https://www.jornada.com.mx/2020/08/10/politica/010n1pol> 07/06/2021
- 38 Ending Violence Against Children and COVID-19 (Child Rights Now!, 2020) Accessed from: [https://www.wvi.org/sites/default/files/2020-07/2020\\_06\\_JF\\_CRN\\_Ending%20Violence%20Against%20Children%20and%20COVID%2019%20ENG.pdf](https://www.wvi.org/sites/default/files/2020-07/2020_06_JF_CRN_Ending%20Violence%20Against%20Children%20and%20COVID%2019%20ENG.pdf) 07/06/2021
- 39 COVID-19 Conversations: The Crisis of Online Child Sexual Exploitation (Equality Now, 2020) Accessed from: [https://www.equalitynow.org/covid\\_19\\_online\\_exploitation](https://www.equalitynow.org/covid_19_online_exploitation) 07/06/2021
- 40 Keeping Children Safe in Uganda's COVID-19 Response (Save the Children, 2020) Accessed from: <https://resourcecentre.savethechildren.net/node/17615/pdf/Joining%20Forces%20-%20Protecting%20children%20during%20Covid-19%20in%20Uganda.pdf> 08/06/2021
- 41 La violencia contra los niños aumenta con la covid (Inter Press Service, 2021) Accessed from: <https://ipsnoticias.net/2021/04/la-violencia-los-ninos-aumenta-la-covid/> 11/06/2021
- 42 Child Sexual Exploitation Materials Hotline Annual Report 2020 (EOKM, 2021) Accessed from: <https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarverslag-2020-DEF-ENG.pdf> 17/06/2021
- 43 National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received by email from the NCA, 25/05/2021
- 44 Pedophilia and Sexual Offending Against Children: Theory, Assessment, and Intervention, Second Edition (Michael Seto, 2018)
- 45 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: [https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm\\_source=ActiveCampaign&utm\\_medium=email&utm\\_content=New+briefings+and+reports+from+the+Alliance+and+our+members&utm\\_campaign=May+2021+newsletter](https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+from+the+Alliance+and+our+members&utm_campaign=May+2021+newsletter) 07/06/2021
- 46 IWF Annual Report 2020: Hidden Services (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other/hidden> 07/06/2021

- 47 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-20/04/2021>
- 48 Why Children are at risk of sexual exploitation during COVID-19 (ECPAT International, 2020) Accessed from: <https://ecpat.exposure.co/covid19?embed=true> 07/06/2021
- 49 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-20/04/2021>
- 50 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-4/> 06/05/2021
- 51 COVID-19 to add as many as 150 million extreme poor by 2021 (World Bank, 2020) Accessed from: <https://www.worldbank.org/en/news/press-release/2020/10/07/covid-19-to-add-as-many-as-150-million-extreme-poor-by-2021> 06/07/2021
- 52 Joint Leaders' statement – Violence against children: A hidden crisis of the COVID-19 pandemic (World Health Organisation, 2020) Accessed from: <https://www.who.int/news/item/08-04-2020-joint-leader-s-statement--violence-against-children-a-hidden-crisis-of-the-covid-19-pandemic> 07/06/2021
- 53 Children's screen time has soared in the pandemic, alarming parents and researchers (NY Times, 2021) Accessed from: <https://www.nytimes.com/2021/01/16/health/covid-kids-tech-use.html> 16/07/2021
- 54 Children at increased online risk during COVID-19 pandemic (UNICEF, 2020) Accessed from: <https://www.unicef.org/bhutan/press-releases/children-increased-online-risk-during-covid-19-pandemic> 16/07/2021
- 55 The impact of the coronavirus pandemic on child welfare: sexual abuse (NSPCC, 2020) Accessed from: <https://learning.nspcc.org.uk/media/2280/impact-of-coronavirus-pandemic-on-child-welfare-sexual-abuse.pdf> 16/07/2021
- 56 Aumentan casos de abuso infantil tras relajarse medidas en Paraguay (Prensa Latina, 2021) Accessed from: <https://www.prensa-latina.cu/index.php?o=rn&id=437283> 07/06/2021
- 57 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: [https://reliefweb.int/sites/reliefweb.int/files/resources/A\\_HRC\\_46\\_31\\_E.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf) 07/06/2021
- 58 Child protection in the time of COVID-19 (Australian Institute of Health and Welfare, 2021) Accessed from: <https://www.aihw.gov.au/reports/child-protection/child-protection-in-the-time-of-covid-19/summary> 16/06/2021
- 59 Protecting children from violence in the time of COVID-19: Disruptions in prevention and response services (Unicef, 2020) Accessed from: <https://www.unicef.org/reports/protecting-children-from-violence-covid-19-disruptions-in-prevention-and-response-services-2020> 07/06/2021
- 60 Netclean Annual Report; Insight 5: COVID-19 has affected the capacity to investigate child sexual abuse crimes (Netclean, 2021) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-5/> 07/06/2021
- 61 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 62 States divert funds, cut expenditure to foot COVID-19 bill (Economic Times, 2021) Accessed from: <https://economic-times.indiatimes.com/news/india/states-divert-funds-cut-expenditure-to-foot-covid-19-bill/articleshow/82448577.cms?from=mdr> 07/06/2021
- 63 Policy Responses to COVID-19: Iraq (International Monetary Fund, 2021) Accessed from: <https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19#top> 07/06/2021
- 64 UK's drastic cut to overseas aid risks future pandemics, say Sage experts (Guardian, 2021) Accessed from: <https://www.theguardian.com/education/2021/mar/20/uks-drastic-cut-to-overseas-aid-risks-future-pandemics-say-sage-experts> 16/07/2021
- 65 100+ Internet Statistics and Facts for 2021 (Website Hosting Rating, 2021) Accessed from: <https://www.websitehostingrating.com/internet-statistics-facts/> 29/04/2021
- 66 Worldwide digital population as of January 2021 (Statista, 2021) Accessed from: <https://www.statista.com/statistics/617136/digital-population-worldwide/> 29/04/2021
- 67 In-depth analysis of changes in world internet performance (GSMA, 2019) Accessed from: <https://www.gsma.com/membership/resources/in-depth-analysis-of-changes-in-world-internet-performance-using-the-speedtest-global-index/> 29/04/2021
- 68 Number of mobile devices worldwide 2020-2024 (Statista, 2020) Accessed from: <https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/> 29/04/2021
- 69 Children in a digital world (Unicef, 2017) Accessed from: <https://www.unicef.org/media/48601/file> 29/04/2021
- 70 Africa Is the Next Frontier For The Internet (Forbes, 2020) accessed from: <https://www.forbes.com/sites/miri-amtuerk/2020/06/09/africa-is-the-next-frontier-for-the-internet/?sh=e8ecd3b49001> 04/05/2021
- 71 Strong mobile growth predicted for sub-Saharan Africa (Connecting Africa, 2020) Accessed from: [http://www.connectingafrica.com/author.asp?section\\_id=761&doc\\_id=764310](http://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310) 04/05/2021

- 72 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: [https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety\\_Report.pdf](https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf) 02/04/2021
- 73 Mobile technology the key to bringing 'education to all', says UN Broadband Commission (Unesco, 2014) Accessed from: <https://en.unesco.org/news/mobile-technology-key-bringing-education-all-says-broadband-commission> 14/05/2021
- 74 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 75 The Internet of Toys: Implications of increased connectivity and convergence of physical and digital play in young children (LSE, 2017) Accessed from: <https://blogs.lse.ac.uk/parenting4digitalfuture/2017/07/19/the-internet-of-toys-implications-of-increased-connectivity-and-convergence-of-physical-and-digital-play-in-young-children/> 20/07/2021
- 76 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: <https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/> 15/07/2021
- 77 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242> 16/02/2021
- 78 Growing up in a connected world (UNICEF, 2019) Accessed from: <https://www.unicef-irc.org/publications/pdf/GK0%20Summary%20Report.pdf> 30/04/2021
- 79 Child and adolescent pornography exposure (Hornor, 2020) Accessed from: [https://www.jpedhc.org/article/S0891-5245\(19\)30384-0/fulltext](https://www.jpedhc.org/article/S0891-5245(19)30384-0/fulltext) 30/04/2021
- 80 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)
- 81 Action to End Child Sexual Abuse and Exploitation (UNICEF, 2020) p.50 Accessed from: <https://www.unicef.org/media/89026/file/CSAE-Report.pdf> 17/05/2021
- 82 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 83 Growing up in a connected world (UNICEF, 2019) Accessed from: <https://www.unicef-irc.org/publications/pdf/GK0%20Summary%20Report.pdf> 30/04/2021
- 84 Impact of online and offline child sexual abuse: "Everyone deserves to be happy and safe" (NSPCC, 2017) Accessed from: <https://learning.nspcc.org.uk/research-resources/2017/impact-online-offline-child-sexual-abuse> 17/05/2021
- 85 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: <https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/> 15/07/2021
- 86 How Everyone's Invited's 'rape culture' claims sparked a #MeToo movement in UK schools (Evening Standard, 2021) Accessed from: <https://www.standard.co.uk/insider/everyones-invited-rape-culture-metoo-movement-schools-b925924.html> 18/05/2021
- 87 #MeToo in school: too many children are sexually harassed by classmates (The Guardian, 2018) Accessed from: <https://www.theguardian.com/commentisfree/2018/feb/11/metoo-school-children-teens-sexual-harassment> (18/05/2021)
- 88 Everyone's Invited (Everyone's Invited, 2020) Accessed from: <https://www.everyonesinvited.uk/> 18/05/2021
- 89 Children and parents: Media use and attitudes report 2019 (Ofcom, 2019) Accessed from: [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0023/190616/children-media-use-attitudes-2019-report.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf) 18/05/2021
- 90 PA Consulting Engagement with Edward Dixon (Rigr AI), 18/03/2021
- 91 'End Online Violence: Learnings from Sri Lanka' Conference (End Violence Against Children, 25/02/2021)
- 92 Darknet Cybercrime Threats to South East Asia (UNODC, 2021) Accessed from: [https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet\\_Cybercrime\\_Threats\\_to\\_Southeast\\_Asia\\_report.pdf](https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf) 29/04/2021
- 93 PA Consulting engagement with Interpol, 25/03/2021
- 94 Interpol: International police coordination required to combat global cyberthreats (CSO, 2021) Accessed from: <https://www.csoonline.com/article/3624992/interpol-international-police-coordination-required-to-combat-global-cyberthreats.html> 20/07/2021
- 95 Child sexual abuse material: Model legislation and global review (ICMEC, 2021) Accessed from: <https://www.icmec.org/csam-model-legislation/> 29/04/2021
- 96 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021
- 97 PA Consulting engagement with Europol, 17/03/2021
- 98 'Legality of Child Pornography' (Wikipedia, 2021) Accessed from: [https://en.wikipedia.org/wiki/Legality\\_of\\_child\\_pornography](https://en.wikipedia.org/wiki/Legality_of_child_pornography) 17/05/2021
- 99 PA Consulting engagement with United States Department of Justice, 22/03/2021

- 100 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/887349/Safer\\_technology\\_\\_safer\\_users-\\_The\\_UK\\_as\\_a\\_world-leader\\_in\\_Safety\\_Tech.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf) 18/05/2021
- 101 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021
- 102 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021
- 103 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: [https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety\\_Report.pdf](https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf) 2/4/2021
- 104 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: [https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety\\_Report.pdf](https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf) 2/4/2021
- 105 Metadata-based detection of child sexual abuse material (Periera, Dodhia and Brown, 2020) Accessed from: <https://arxiv.org/pdf/2010.02387.pdf> 29/04/2021
- 106 PA Consulting engagement with Terre des Hommes, 25/02/2021
- 107 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/887349/Safer\\_technology\\_\\_safer\\_users-\\_The\\_UK\\_as\\_a\\_world-leader\\_in\\_Safety\\_Tech.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf) 18/05/2021
- 108 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021
- 109 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021
- 110 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf> 02/06/2021
- 111 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8> 06/05/2021
- 112 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 113 Germany's Network Enforcement Act and its impact on social networks (Taylor Wessing, 2018) Accessed from: <https://www.taylorwessing.com/download/article-germany-nfa-impact-social.html> 10/06/21
- 114 Email received from the Office of the e-Safety Commissioner, 13/07/2021
- 115 UK to introduce world first online safety laws (GOV.UK, 2019) Accessed from: <https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws> 10/06/2021
- 116 The EU unveils its plan to rein in big tech (Economist, 2020) Accessed from: <https://www.economist.com/business/2020/12/15/the-eu-unveils-its-plan-to-rein-in-big-tech> 10/06/2021
- 117 Online Safety and Media Regulation Bill (GOV.IE, 2020) Accessed from: <https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/> 10/06/2021
- 118 Communication from the Commission to the European parliament, the council, the European economic and Social Committee and the Committee of the Regions: EU Strategy for a more effective fight against child sexual abuse (European Commission, 2020) Accessed from: [https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724\\_com-2020-607-commission-communication\\_en.pdf](https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf) 10/06/2021
- 119 End-to-End Encryption: Understanding the impacts for child safety online (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 10/06/2021
- 120 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: [https://www.unicef-irc.org/publications/pdf/Encryption\\_privacy\\_and\\_children%E2%80%99s\\_right\\_to\\_protection\\_from\\_harm.pdf](https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf) 21/07/2021
- 121 Google is testing end-to-end encryption in android messages (Wired, 2020) Accessed from: <https://www.wired.com/story/google-is-testing-end-to-end-encryption-in-android-messages/> 10/06/2021
- 122 NSPCC urges Facebook to stop encryption plans (BBC News, 2020) Accessed from: <https://www.bbc.co.uk/news/technology-51391301> 10/06/2021
- 123 End-to-End Encryption (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 25/05/2021
- 124 Briefing on the future of digital tools to detect child sexual exploitation and abuse online in Europe (WeProtect Global Alliance, 2021) Accessed from: <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/600086ba8f-223010c1b4b756/1610647258029/WPGA+European+ePrivacy+briefing+Jan+21.pdf> 10/06/2021
- 125 A battle won, but not the war in the global fight for child safety (NCMEC, 2021) Accessed from: <https://www.missingkids.org/childsafetyfirst#:~:text=As%20NCMEC%20has%20recently%20reported%2C%20we%20have%20seen,to%20offer%20permanent%20solutions%20for%20child%20safety%20online.> 10/06/2021



- 126 Provisional agreement on temporary rules to detect and remove online child abuse (News, European Parliament, 2021) Accessed from: <https://www.europarl.europa.eu/news/en/press-room/20210430IPRO3213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse> 22/06/2021
- 127 Project Beacon: EU comes to political agreement to continue the use of online tools against CSAM (ECPAT, 2021) Accessed from: <https://www.ecpat.org/news/tag/project-beacon/> 21/07/2021
- 128 The EU Strategy on the Rights of the Child and the European Child Guarantee (European Commission, 2021) Accessed from: The EU Strategy on the Rights of the Child and the European Child Guarantee | European Commission (europa.eu) 21/07/2021
- 129 Fighting against child sexual abuse: join the stakeholder consultation (European Commission, 2021) Accessed from: [https://ec.europa.eu/home-affairs/news/fighting-against-child-sexual-abuse-join-stakeholder-consultation\\_en](https://ec.europa.eu/home-affairs/news/fighting-against-child-sexual-abuse-join-stakeholder-consultation_en) 21/07/2021
- 130 NCMEC's Statement Regarding End-to End Encryption (NCMEC, 2019) Accessed from: <https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption> 10/06/2021
- 131 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: [https://www.unicef-irc.org/publications/pdf/Encryption\\_privacy\\_and\\_children%E2%80%99s\\_right\\_to\\_protection\\_from\\_harm.pdf](https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf) 21/07/2021
- 132 Statement on end-to-end encryption and public safety (Australian Government Department of Home Affairs, 2021) Shared by the Australian Department of Home Affairs by email, 19/05/2021
- 133 VGT position on End-to-End Encryption (Virtual Global Taskforce, 2021) Received via email from the NCA on 14/06/2021
- 134 NCA National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received via email from the NCA on 25/05/2021
- 135 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 136 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: <https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse> 10/06/2021
- 137 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 138 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 139 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: <https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse> 10/06/2021
- 140 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: [https://www.unicef-irc.org/publications/pdf/Encryption\\_privacy\\_and\\_children%E2%80%99s\\_right\\_to\\_protection\\_from\\_harm.pdf](https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf) 21/07/2021
- 141 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 142 End-to-End Encryption (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 25/05/2021
- 143 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: [https://www.unicef-irc.org/publications/pdf/Encryption\\_privacy\\_and\\_children%E2%80%99s\\_right\\_to\\_protection\\_from\\_harm.pdf](https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf) 21/07/2021
- 144 Project Arachnid: Online Availability of Child Sexual Abuse Material (Canadian Centre for Child Protection, 2021) Accessed from: <https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/> 10/06/2021
- 145 Webinar: The Online Harms Bill – more harm than good? (11KBW, 20/05/2021)
- 146 Protection of children should always trump protection of privacy (Julie Inman Grant, eSafety Commissioner, 2020) Accessed from: <https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy> 10/06/2021
- 147 The Decentralised Web of Hate: White Supremacists are starting to use peer-to-peer technology; are we prepared? (Rebellious Data LLC, 2020) Accessed from: <https://rebellious-data.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf> 10/06/2021
- 148 Messaging services are providing a more private internet (Economist, 2021) Accessed from: <https://www.economist.com/international/2021/01/23/messaging-services-are-providing-a-more-private-internet> 10/06/2021
- 149 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf> 02/06/2021
- 150 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2020) Accessed from: <https://www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/> 10/06/2021
- 151 Tech giants list principles for handling harmful content (Axios, 2021) Accessed from: <https://www.axios.com/tech-giants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html> 10/06/2021
- 152 The Technology Coalition Announces Project Protect (Technology Coalition, 2020) Accessed from: <https://www.technology-coalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/> 24/06/2021

- 153 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: <https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020> 24/02/2021
- 154 Online enticement (NCMEC) Accessed from: <https://www.missingkids.org/netsmartz/topics/onlineenticement> 19/04/2021
- 155 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: <https://www.netclean.com/net-clean-report-2020/insight-2/> 26/01/2021
- 156 Trends identified in CyberTipline sextortion reports (NetClean, 2016) Accessed from: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf> 01/03/2021
- 157 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: [https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety\\_Report.pdf](https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf) 02/04/2021
- 158 Out of the Shadows (Economist Impact, 2018) Accessed from: <https://outoftheshadows.eiu.com/> 25/01/2021
- 159 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: [https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children\\_FINAL\\_9-18-17.pdf](https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf) 04/02/2021
- 160 Kids & Tech: Evolution of Today's Digital Natives (Influence Central, 2017) Accessed from: <https://influence-central.com/trendspotting/launching-the-new-influence-central-trend-report> 12/04/2021
- 161 Technology working group report (Child Dignity Foundation, 2018) Accessed from: <https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf> 26/02/2021
- 162 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 163 Online grooming: What it is, how it happens, and how to defend children (Thorn, 2020) Accessed from: <https://www.thorn.org/blog/online-grooming-what-it-is-how-it-happens-and-how-to-defend-children/> 07/04/2021
- 164 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: <https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf> 10/03/2021
- 165 Trends identified in cyberipline sextortion reports (NetClean, 2016) Accessed from: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf> 01/03/2021
- 166 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: <https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf> 11/03/2021
- 167 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: <https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation> 28/01/2021
- 168 COVID-19 accelerates global video gaming market to \$170bn (Consultancy-me.com, 2020) Accessed from: <https://www.consultancy-me.com/news/3041/covid-19-accelerates-global-gaming-market-to-170-billion> 16/02/2021
- 169 The Marie Collins Foundation, Accessed from: <https://www.mariecollinsfoundation.org.uk/> 29/04/2021
- 170 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 171 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: [https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children\\_FINAL\\_9-18-17.pdf](https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf) 04/02/2021
- 172 Safety-by-design overview (eSafety Commissioner, 2019) Accessed from: <https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf> 11/02/2021
- 173 Digital Age Assurance Tools and Children's Rights Online across the Globe (UNICEF, 2021) Accessed from: <https://www.unicef.org/media/97461/file/Digital%20Age%20Assurance%20Tools%20and%20Children%E2%80%99s%20Rights%20Online%20across%20the%20Globe.pdf> 07/05/2021
- 174 Video games and online chats are 'hunting grounds' for sexual predators (New York Times, 2019) Accessed from: <https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html> 21/04/2021
- 175 Case study submission from TikTok, received on 10/05/2021
- 176 Continuing to Make Instagram Safer for the Youngest Members of Our Community (Instagram, 2021) Accessed from: <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community> 21/04/2021
- 177 What is a supervised experience on YouTube? (Google, 2021) Accessed from: <https://support.google.com/youtube/answer/10314940?hl=en> 20/07/2021
- 178 Perpetrators of sexual violence: statistics (RAINN) Accessed from: <https://www.rainn.org/statistics/perpetrators-sexual-violence> 16/04/2021
- 179 The sexual exploitation and abuse of deaf and disabled children online (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/Intelligence-briefing-2021-The-sexual-exploitation-and-abuse-of-disabled-children.pdf> 23/02/2021

- 180 Ending violence against children: key messages and statistics (End Violence Against Children) [https://www.end-violence.org/sites/default/files/paragraphs/download/Key Messages\\_Long\\_0.pdf](https://www.end-violence.org/sites/default/files/paragraphs/download/Key_Messages_Long_0.pdf) 12/04/2021
- 181 CyberTipline: 2019 & 2020 Reports by country (NCMEC, 2020) accessed from: <https://www.missingkids.org/gethelp-now/cybertipline> 19/04/2021
- 182 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: [https://www.ijm.org/documents/studies/Final-Public-Full-Report-5\\_20\\_2020.pdf](https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf) 17/02/2021
- 183 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 184 IWF Annual Report: International Overview (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/overview> 21/04/2021
- 185 Self-generated child sexual abuse (IWF Annual Report, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 29/07/2021
- 186 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: [https://reliefweb.int/sites/reliefweb.int/files/resources/A\\_HRC\\_46\\_31\\_E.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf) 04/03/2021
- 187 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: <https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimas-en-lo-corrido-de-2021> 11/03/2021
- 188 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: <https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/> 25/02/2021
- 189 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: [https://www.aic.gov.au/sites/default/files/2021-02/ti616\\_production\\_and\\_distribution\\_of\\_child\\_sexual\\_abuse\\_material\\_by\\_parental\\_figures.pdf](https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf) 09/03/2021
- 190 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: <https://protect-eu.mimecast.com/s/WuEPCWn-WgFxLBY3Hxchqm?domain=levante-emv.com> 23/02/2021
- 191 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: [https://www.aic.gov.au/sites/default/files/2021-02/ti616\\_production\\_and\\_distribution\\_of\\_child\\_sexual\\_abuse\\_material\\_by\\_parental\\_figures.pdf](https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf) 09/03/2021
- 192 Online enticement of children: an in-depth analysis of CyberTipline reports (National Center for Missing and Exploited Children, 2017) Accessed from: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf> 11/02/2021
- 193 The cycle of child sexual abuse stops now (Project Arachnid) Accessed from: <https://projectarachnid.ca/en/07/04/2021>
- 194 PA Consulting engagement with United States Department of Justice, 22/03/2021
- 195 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021
- 196 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 197 Child abuse predator 'handbook' lists ways to target children during coronavirus lockdown (The Guardian, 2020) Accessed from: <https://www.theguardian.com/society/2020/may/14/child-abuse-predator-handbook-lists-ways-to-target-children-during-coronavirus-lockdown> 23/02/2021
- 198 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 199 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021
- 200 South Korea confronts its voyeurism epidemic (The Guardian, 2018) Accessed from: <https://www.theguardian.com/world/2018/jul/03/a-part-of-daily-life-south-korea-confronts-its-voyeurism-epidemic-sexual-harassment> 08/03/2021
- 201 Netclean Report 2019: A report about child sexual abuse crime (Netclean, 2019) Accessed from: <https://www.netclean.com/netclean-report-2019/> 28/01/2021
- 202 A deepfake porn bot is being used to abuse thousands of women (WIRED, 2020) Accessed from: <https://www.wired.co.uk/article/telegram-deepfakes-deepnude-ai> 19/03/2021
- 203 Cybersex, erotic tech and virtual intimacy are on the rise during COVID-19 (The Conversation, 2020) Accessed from: <https://theconversation.com/cybersex-erotic-tech-and-virtual-intimacy-are-on-the-rise-during-covid-19-141769> 19/03/2021
- 204 Immersive Technologies – Position Statement (e-Safety Commissioner, 2021) Accessed from: <https://www.esafety.gov.au/about-us/tech-trends-and-challenges/immersive-tech> 14/07/2021
- 205 CGI (Computer Generated Imagery) (TechTarget, 2016) Accessed from: <https://whatis.techtarget.com/definition/CGI-computer-generated-imagery> 08/04/2021
- 206 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: [https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines\\_en.pdf](https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf) 17/03/2021

- 207 What is deepfake? (Business Insider, 2021) Accessed from: <https://www.businessinsider.com/what-is-deep-fake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20re-corded%20video> 08/04/2021
- 208 PA Consulting engagement with Terre des Hommes, 25/02/2021
- 209 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT France, 2017) Accessed from: [https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE\\_ANG-min.pdf](https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf) 09/08/2021
- 210 Non-photographic visual depictions (Internet Watch Foundation, 2007) Accessed from: <https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depic-tions> 17/03/2021
- 211 Child Sexual Abuse Material: Model Legislation and Global Review (International Center for Missing and Exploited Children, 2018) Accessed from: <https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf> 05/03/2021
- 212 Computer-generated 'Sweetie' catches online predators (BBC News, 2013) Accessed from: <https://www.bbc.co.uk/news/uk-24818769> 08/03/2021
- 213 Child sexual abuse in the digital era: Rethinking legal frameworks and transnational law enforcement collaboration (Universiteit Leiden, 2020) Accessed from: <https://scholarly-publications.universiteitleiden.nl/access/item%3A2966712/view> 07/05/2021
- 214 National Strategic Assessment of Serious and Organised Crime 2020 (National Crime Agency, 2020) Accessed from: <https://www.nationalcrimeagency.gov.uk/news/nsa2020> 24/03/2021
- 215 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-vic-tims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 216 PA Consulting engagement with Interpol, 25/03/2021
- 217 PA Consulting engagement with Ethel Quayle, 04/03/2021
- 218 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: <https://www.iicsa.org.uk/publications/investigation/internet> 02/02/2021
- 219 Internet Organised Crime Threat Assessment (IOCTA) 2020 (Europol, 2020) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/internet-organ-ised-crime-threat-assessment-iocta-2020> 30/03/2021
- 220 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/euro-pean-union-serious-and-organised-crime-threat-assessment> 20/04/2021
- 221 Child Rescue Coalition (CRC): Protecting Innocence Through Technology (CRC, 2021) Email received from CRC, 30/03/2021
- 222 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 26/01/2021
- 223 Hackers leaked 22 million records on the dark web in 2020 (ID Agent, 2020) Accessed from: <https://www.idagent.com/hackers-leaked-22-million-records-on-the-dark-web-in-2020> 29/04/2021
- 224 Trends in Online Child Sexual Abuse Material (ECPAT, 2017) Accessed from: <https://www.ecpat.org/wp-content/up-loads/2016/05/Emerging-Issues-and-Global-Threats-Child-ren-online-2017-1.pdf> 25/03/2021
- 225 COVID-19: Child Sexual Exploitation (Europol, 2020) Ac-cessed from: <https://www.europol.europa.eu/covid-19/cov-id-19-child-sexual-exploitation> 20/04/2021
- 226 Brave.com now has its own Tor onion service, providing more users with secure access to Brave (Brave.com, 2020) Accessed from: <https://brave.com/new-onion-service/> 20/04/20
- 227 Tor (Investopedia, 2019) Accessed from: <https://www.investo-pedia.com/terms/t/tor.asp> 07/05/2021
- 228 PA Consulting engagement with United States Department of Justice, 07/04/2021 NCMEC Engagement
- 229 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021
- 230 PA Consulting engagement with United States National Centre for Missing and Exploited Children, 16/03/2021
- 231 Millions of attempts to access child sexual abuse online during lockdown (Internet Watch Foundation, 2020) Accessed from: <https://www.iwf.org.uk/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown> 08/02/2021
- 232 COVID-19 conversations: The Crisis of Online Child Exploita-tion (Equality Now, 2021) Accessed from: [https://www.equali-tynow.org/covid\\_19\\_online\\_exploitation](https://www.equali-tynow.org/covid_19_online_exploitation) 07/06/2021
- 233 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: [https://reliefweb.int/sites/reliefweb.int/files/resources/A\\_HRC\\_46\\_31\\_E.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf) 04/03/2021
- 234 The Motivation-Facilitation Model of Sexual Offending (Michael C. Seto, 2017) Accessed from: <https://journals.sagepub.com/doi/full/10.1177/1079063217720919> 29/07/2021
- 235 Internet Sex Offenders (Seto, Michael C., 2013)
- 236 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBAR-GO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021

- 237 Sexual interests of child sexual exploitation material (CSEM) consumers (Fortin and Proulx, 2018) Accessed from: <https://journals.sagepub.com/doi/10.1177/0306624X18794135> 11/02/2021
- 238 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 239 How extreme porn has become a gateway drug into child abuse (The Guardian, 2020) Accessed from: <https://www.theguardian.com/global-development/2020/dec/15/how-extreme-porn-has-become-a-gateway-drug-into-child-abuse> 15/02/2021
- 240 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Prichard, Wortley, Waters, Spiranovic, Hunn, Krone, 2020) Received from Donald Findlater (Lucy Faithfull Foundation), 16/02/2021
- 241 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242> 16/02/2021
- 242 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)
- 243 On Youtube's Digital Playground, an Open Gate for Pedophiles (The New York Times, 2019) Accessed from: <https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html?module=inline> 04/03/2021
- 244 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 245 On Youtube, a network of paedophiles is hiding in plain sight (WIRED, 2019) Accessed from: <https://www.wired.co.uk/article/youtube-pedophile-videos-advertising> 31/03/2021
- 246 Barriers Abusers Overcome In Order To Abuse (Psychology Tools) Accessed from: <https://www.psychologytools.com/resource/barriers-abusers-overcome-in-order-to-abuse/> 29/03/2021
- 247 Child Sexual Abuse (Finkelhor, 1984)
- 248 The Four Rs of Responsibility, Part 1: Removing Harmful Content (Youtube, 2019) Accessed from: <https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-remove/> 27/07/2021
- 249 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (NatCen Social Research, 2017) Accessed from: <https://natcen.ac.uk/media/1535277/Behaviours-and-characteristics-of-perpetrators-of-online-facilitated-child-sexual-abuse-and-exploitation.pdf> 09/02/2021
- 250 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 251 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: [https://www.ijm.org/documents/studies/Final-Public-Full-Report-5\\_20\\_2020.pdf](https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf) 23/02/2021
- 252 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Pritchard et al., 2020)
- 253 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 254 Ground-breaking research on perpetrator prevention (Oak Foundation, 2021) Accessed from: <https://oakfnd.org/groundbreaking-research-on-perpetration-prevention/> 13/07/2021
- 255 IWF Annual Report: About Our Year (IWF, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/about/year/ceo> 21/04/2021
- 256 Game-changing chatbot to target people trying to access child sexual abuse online (IWF, 2020) Accessed from: <https://www.iwf.org.uk/news/game-changing%E2%80%99-chatbot-to-target-people-trying-to-access-child-sexual-abuse-online> 20/04/2021
- 257 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 258 Suojellaan Lapsia, Accessed from: <https://suojellaanlapsia.fi/> 29/04/2021
- 259 COVID-19 and Missing and Exploited Children (NCMEC, 2021) Accessed from: <https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children> 22/04).
- 260 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends> 22/04/2021
- 261 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 262 PA Consulting engagement with NCMEC, 16/03/2021
- 263 PA Consulting Engagement with NCMEC, 22/04/2021
- 264 IWF Annual Report: Site types analysis (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/sitetypes> 22/04/2021

- 265 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: <https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation> 28/01/2021
- 266 PA Consulting engagement with Interpol, 25/03/2021
- 267 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden> 22/04
- 268 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/glossary> 10/05/2021
- 269 How child sexual abuse material is stored (Netclean, 2019) Accessed from: <https://www.netclean.com/netclean-report-2019/insight-4/> 22/04/2021
- 270 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 271 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021
- 272 PA Consulting engagement with United States Department of Justice, 22/03/2021
- 273 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021
- 274 Preventing Child Exploitation on our Apps (Facebook, 2020) Accessed from: <https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/#:~:text=Using%20our%20apps%20to%20harm,authorities%20to%20keep%20children%20safe.> 22/04/2021
- 275 Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims (Thorn, 2018) Accessed from: [https://www.missingkids.org/content/dam/missing-kids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM\\_FullReport\\_FINAL.pdf](https://www.missingkids.org/content/dam/missing-kids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf) 15/07/2021
- 276 Study on the effects of new information technologies on the abuse and exploitation of children (United Nations Office on Drugs and Crime, 2015) Accessed from: [https://www.unodc.org/documents/Cybercrime/Study\\_on\\_the\\_Effects.pdf](https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf) 22/04/2021
- 277 Crime investigations of 'child abuse material' - Challenges and opportunities posed by digital technology (Marie Eneman, 2020) Accessed from: [https://www.researchgate.net/publication/344072738\\_Crime\\_investigations\\_of\\_'child\\_abuse\\_material'\\_-\\_Challenges\\_and\\_opportunities\\_posed\\_by\\_digital\\_technology](https://www.researchgate.net/publication/344072738_Crime_investigations_of_'child_abuse_material'_-_Challenges_and_opportunities_posed_by_digital_technology) 10/05/2021
- 278 Production of child sexual abuse material by parental figures (Australian Government, Institute of Criminology, 2021) Accessed from: [https://www.aic.gov.au/sites/default/files/2021-02/ti616\\_production\\_and\\_distribution\\_of\\_child\\_sexual\\_abuse\\_material\\_by\\_parental\\_figures.pdf](https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf) 16/07/2021
- 279 Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers (Facebook Research, 2021) Accessed from: <https://research.fb.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/> 29/06/2021
- 280 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Commercial> 22/04/2021
- 281 IWF Annual Report: Domain analysis (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/domain> 22/04/2021
- 282 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Commercial> 22/04/2021
- 283 Cryptocurrency and the trade of online child sexual abuse material (ICMEC, 2021) Accessed from: [https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material\\_03.17.21-publish-1.pdf](https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf) 22/04/21
- 284 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other> 22/04/2021
- 285 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other> 22/04/2021
- 286 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other> 22/04/2021
- 287 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: <https://www.netclean.com/2018/10/30/hash-values/> 22/04/2021
- 288 International Child Sexual Exploitation Database (INTERPOL, 2018) Accessed from: <https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database> 22/04/2021
- 289 IWF Annual Report: Hidden Services (IWF, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other/hidden> 10/05/2021
- 290 IWF Annual Report: Geographical hosting (IWF, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/geographic> 10/05/2021
- 291 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 292 PA Consulting engagement with IWF, 01/03/2021
- 293 PA Consulting engagement with Interpol, 25/03/2021
- 294 PA Consulting engagement with IWF, 01/03/2021
- 295 Technology working group report (Child Dignity Foundation, 2018) Accessed from: <https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf> 26/02/2021
- 296 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: <https://static1.squarespace.com/static/5a4d5d4e7131a5845cd690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf> 22/04/2021

- 297 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021
- 298 IWF Annual Report: Self-generated content study (IWF, 2012) Accessed from: <https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202012%20Annual%20and%20Charity%20Report%20%28web%29.pdf> 06/05/2021
- 299 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: [https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE\\_ANG-min.pdf](https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf) 22/04/2021
- 300 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 301 PA Consulting engagement with Internet Watch Foundation, 01/03/2021
- 302 Interim code of practice on online child sexual exploitation and abuse (accessible version)(GOV.UK, 2020) Accessed from: <https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual-exploitation-and-abuse-accessible-version> 19/07/2021
- 303 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: [https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia\\_ENG.pdf](https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf) 06/05/2021
- 304 Prevalence of Multiple Forms of Sexting Behaviour Among Youth (Madigan et al., 2018) Accessed from: <https://jamanetwork.com/journals/jamapediatrics/fullarticle/2673719?resultClick=1> 06/05/2021
- 305 'Staying Safe Online' survey: wat unwanted sexual images are being sent to teenagers on social media? (University College London, 2019) Accessed from: <https://blogs.ucl.ac.uk/ioe/2020/06/19/staying-safe-online-survey-what-unwanted-sexual-images-are-being-sent-to-teenagers-on-social-media/> 20/07/2021
- 306 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021
- 307 IWF Annual Report: Who we are (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/about/us> 11/05/2021
- 308 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 309 An Exploratory Study of Sexting Behaviours Among Heterosexual and Sexual Minority Early Adolescents (Van Ouytsel et al., 2019) Accessed from: <https://pubmed.ncbi.nlm.nih.gov/31473082/> 14/05/2021
- 310 Look at me: Teens, Sexting, and Risks (Internet Matters, 2021) Accessed from <https://www.internetmatters.org/wp-content/uploads/2020/06/Internet-Matters-Look-At-Me-Report-1.pdf> 06/05/2021
- 311 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: <https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf> 06/05/2021
- 312 Online harmful sexual behaviours in children and young people under 18 (eSafety Commissioner, 2020) Accessed from: <https://www.esafety.gov.au/sites/default/files/2020-09/Online%20harmful%20sexual%20behaviours%20Position%20statement.pdf> 13/07/2021
- 313 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 314 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: [https://info.thorn.org/hubfs/Research/08112020\\_SG-CSAM\\_AttitudesExperiences-Report\\_2019.pdf](https://info.thorn.org/hubfs/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf) 28/07/2021
- 315 A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people (NSPCC, Children's Commissioner, Middlesex University London, 2016) Accessed from: <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/MDX-NSPCC-OCC-Online-Pornography-Report.pdf> 28/07/2021
- 316 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021
- 317 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 318 Online Nation: 2021 Report (Ofcom, 2021) Accessed from: [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0013/220414/online-nation-2021-report.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf) 24/06/2021
- 319 Faster Takedown of Online Sexual Abuse Sought (Manila-Standard.Net, 2021) Accessed from: <https://manilastandard.net/mobile/article/349129> 06/05/2021
- 320 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: [https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia\\_ENG.pdf](https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf) 06/05/2021
- 321 The children selling explicit videos on OnlyFans (BBC News, 2021) Accessed from: <https://www.bbc.co.uk/news/uk-57255983> 07/07/2021
- 322 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-4/> 06/05/2021

- 323 'Grave threat' to children from predatory internet groomers as online child sexual abuse material soars to record levels (IWF, 2021) Accessed from: <https://www.iwf.org.uk/news/%E2%80%98grave-threat%E2%80%99-children-predatory-internet-groomers-online-child-sexual-abuse-material-soars> 07/05/2021
- 324 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: <https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf> 06/05/2021
- 325 Emerging Patterns and Trends Report: Online-Produced Sexual Content (IWF, 2015) p.3 Accessed from: [https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced\\_sexual\\_content\\_report\\_100315.pdf](https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf) 19/05/2021
- 326 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: [https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020\\_SG-CSAM\\_AttitudesExperiences-Report\\_2019.pdf?\\_\\_hstc=208625165.851aa734d938b21fee07aa6d05-bc9e7.1604505256798.1614622415296.1614700924025.7&\\_\\_hssc=208625165.2.1614700924025&\\_\\_hsfp=723267087](https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05-bc9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087) 06/05/2021
- 327 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: <https://www.iicsa.org.uk/publications/investigation/internet> 02/02/2021
- 328 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 329 PA Consulting Engagement with SafeBAE, 02/03
- 330 SafeToNet acquires German mobile phone stores to safeguard children online (PR Newswire, 2021) Accessed from: <https://www.prnewswire.com/news-releases/safetonet-acquires-german-mobile-phone-stores-to-safeguard-children-online-301247334.html> 14/05/2021
- 331 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: [https://www.coe.int/t/e/treaties/Convention\\_on\\_the\\_Protection\\_of\\_Children\\_Against\\_Sexual\\_Exploitation\\_and\\_Sexual\\_Abuse/1680a069f8](https://www.coe.int/t/e/treaties/Convention_on_the_Protection_of_Children_Against_Sexual_Exploitation_and_Sexual_Abuse/1680a069f8) (coe.int) 06/05/2021
- 332 Teen sexting is decriminalised between partners of similar age (news.com.au, 2018) Accessed from: <https://www.news.com.au/national/nsw-act/courts-law/teen-sexting-is-decriminalised-between-partners-of-similar-age/news-story/3fdceb4adb2c6028eab1f76a86ba5ab> 06/05/2021
- 333 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Council of Europe, 2007) Accessed from: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/699615/MS4.2018\\_Lanzarote\\_CM9602\\_WEB.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699615/MS4.2018_Lanzarote_CM9602_WEB.pdf) 22/06/2021
- 334 Police Response to Youth Offending Around the Generation and Distribution of Indecent Images of Children and its Implications (University of Suffolk/ Marie Collins Foundation, 2019) Accessed from: [https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Outcome-21\\_2.pdf](https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Outcome-21_2.pdf) 13/05/2021
- 335 Sharing nudes and semi-nudes: advice for education settings working with children and young people (GOV.UK, 2020) Accessed from: <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people> 01/06/2021
- 336 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 337 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 338 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 339 Sexting among high school students in a metropolis in Ghana: an exploratory study (Baiden et al., 2019) Accessed from: <https://www.tandfonline.com/doi/abs/10.1080/17482798.2020.1719854> 07/05/2021
- 340 Sexting: Prevalence, Predictors, and Associated Sexual Risk Behaviors among Postsecondary School Young People in Ibadan, Nigeria (Olatunde and Balogun, 2017) Accessed from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5420550/> 07/05/2021
- 341 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: [https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020\\_SG-CSAM\\_AttitudesExperiences-Report\\_2019.pdf?\\_\\_hstc=208625165.851aa734d938b21fee07aa6d05-bc9e7.1604505256798.1614622415296.1614700924025.7&\\_\\_hssc=208625165.2.1614700924025&\\_\\_hsfp=723267087](https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05-bc9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087) 06/05/2021
- 342 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021
- 343 The reception of sexual messages among young Chileans and Uruguayans (Alfaro et al., 2020) Accessed from: [https://www.researchgate.net/publication/347336149\\_The\\_reception\\_of\\_sexual\\_messages\\_among\\_young\\_Chileans\\_and\\_Uruguayans](https://www.researchgate.net/publication/347336149_The_reception_of_sexual_messages_among_young_Chileans_and_Uruguayans) 28/05/2021
- 344 Online Harms White Paper (UK Government, 2019) Accessed from: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/973939/Online\\_Harms\\_White\\_Paper\\_V2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf) 07/05/2021



- 345 Teenage Sexting and Sexual Behaviours in an Iranian Setting (Ghorashi, 2019) Accessed from: [https://www.researchgate.net/publication/333826458\\_Teenage\\_Sexting\\_and\\_Sexual\\_Behaviors\\_in\\_an\\_Iranian\\_Setting](https://www.researchgate.net/publication/333826458_Teenage_Sexting_and_Sexual_Behaviors_in_an_Iranian_Setting) 19/05/2021
- 346 Demystifying Sexting: Adolescent Sexting and its Associations With Parenting Styles and Sense of Parental Social Control in Israel (Dolev-Cohen and Ricon, 2020) Accessed from: <https://cyberpsychology.eu/article/view/11878/11340> 19/05/2021
- 347 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 348 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse> 26/01/2021
- 349 Safe from harm: Tackling webcam child sexual abuse in the Philippines (UNICEF, 2016) Accessed from: <https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines> 09/08/21
- 350 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: <https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children> 22/04/2021
- 351 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021
- 352 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021
- 353 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: [https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE\\_ANG-min.pdf](https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf) 22/04/2021
- 354 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBAR-GO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021
- 355 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: [https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE\\_ANG-min.pdf](https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf) 22/04/2021
- 356 Victims of livestreamed child sexual abuse (Netclean, 2019) Accessed from <https://www.netclean.com/netclean-report-2019/insight-2/> 22/04/2021
- 357 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 358 UNICEF: What works to prevent online and offline child sexual exploitation and abuse: Review of national education strategies in East Asia and the Pacific (UNICEF, 2020) Accessed from <https://www.sddirect.org.uk/media/1874/what-works-to-prevent-online-and-offline-csae-in-east-asia-and-the-pacific.pdf> 22/04/2021
- 359 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: [https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP\\_2020\\_Chapter5.pdf](https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf) 22/04/2021
- 360 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: [https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP\\_2020\\_Chapter5.pdf](https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf) 22/04/2021
- 361 Impact of the COVID 19 pandemic on trafficking in persons (UNODC, 2021) Accessed from: [https://www.unodc.org/documents/Advocacy-Section/HTMSS\\_Thematic\\_Brief\\_on\\_COVID-19.pdf](https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf) 22/04/2021
- 362 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: [https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP\\_2020\\_Chapter5.pdf](https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf) 22/04/2021
- 363 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment> 20/04/2021
- 364 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021
- 365 Why are human trafficking cases difficult to identify and prosecute (John Vanek, 2018) Accessed from: <https://johnvanek.com/2018/01/25/why-are-human-trafficking-cases-difficult-to-identify-and-prosecute/> 11/05/2021
- 366 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 367 Online sexual exploitation of children in the Philippines (IJM, 2020) Accessed from: [https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5\\_20\\_2020.pdf](https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020.pdf) 22/04/2021
- 368 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: <https://www.icmec.org/wp-content/uploads/2017/05/IC-MEC-FCACPCryptocurrencyPaperFINAL5-17.pdf> 22/04/2021
- 369 Case Study: The Fintel Alliance – a public private partnership (AUSTRAC, 2021) Shared by the Australian Department of Home Affairs, 19/05/2021
- 370 IJM Composite Case Study - 'Follow the Money' – Trafficking for livestreamed Online Child Sexual Exploitation. Received by email 31/03
- 371 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: <https://www.icmec.org/wp-content/uploads/2017/05/IC-MEC-FCACPCryptocurrencyPaperFINAL5-17.pdf> 22/04/2021

- 372 Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence: Public Bulletin (Egmont Group, 2020) Accessed from: [https://egmontgroup.org/sites/default/files/filedepot/20200901\\_CSAE%20Public%20Bulletin.pdf](https://egmontgroup.org/sites/default/files/filedepot/20200901_CSAE%20Public%20Bulletin.pdf) 16/07/2021
- 373 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021
- 374 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: [https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE\\_ANG-min.pdf](https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf) 22/04/2021
- 375 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: <https://static1.squarespace.com/static/5a4d5d4e7131a5845cd-d690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf> 22/04/2021
- 376 Cambodia feared lagging behind predators in cybersex trafficking crackdown (Reuters, 2019) Accessed from: <https://www.reuters.com/article/us-cambodia-sexcrimes-children/cambodia-feared-lagging-behind-predators-in-cybersex-trafficking-crackdown-idUSKCN1VW00B> 22/04/2021
- 377 Informe de monitoreo de país sobre la explotación sexual comercial de niños, niñas y adolescentes (ECPAT, 2014) Accessed from: <https://www.ecpat.org/wp-content/uploads/2016/04/IMP%20MEXICO.pdf> 22/04/2021
- 378 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf> 17/06/2021
- 379 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021
- 380 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: [https://www.who.int/violence\\_injury\\_prevention/resources/publications/en/guidelines\\_chap7.pdf](https://www.who.int/violence_injury_prevention/resources/publications/en/guidelines_chap7.pdf) 25/05/2021
- 381 Glossary on Sexual Exploitation and Abuse (United Nations, 2017) Accessed from: [https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English\\_0.pdf](https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English_0.pdf) 25/05/2021
- 382 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: [https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines\\_en.pdf](https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf) 25/05/2021
- 383 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: [https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines\\_ENG.pdf](https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf) (23/07/2021)
- 384 Child Sexual Abuse Material (NCMEC) Accessed from: <https://www.missingkids.org/theissues/csam> 25/05/2021
- 385 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 386 Non-Photographic Visual Depictions (IWF, 2007) Accessed from: <https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depictions> 25/05/2021
- 387 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: [https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines\\_en.pdf](https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf) 25/05/2021
- 388 Grooming (NSPCC) Accessed from: <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/> 25/05/2021
- 389 Online Enticement (NCMEC) Accessed from: <https://www.missingkids.org/netsmartz/topics/onlineenticement> 25/05/2021
- 390 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: [https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines\\_en.pdf](https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf) 25/05/2021
- 391 What is a deepfake? Everything you need to know about the AI-powered fake media (Business Insider, 2021) Accessed from: <https://www.businessinsider.com/what-is-deepfake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20recorded%20video.> 25/05/2021
- 392 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 393 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)
- 394 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: [https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines\\_en.pdf](https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf) 25/05/2021
- 395 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 396 Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (United Nations, 2000) Accessed from: <https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx>
- 397 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021

- 398 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 399 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 400 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 401 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 402 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/887349/Safer\\_technology\\_\\_safer\\_users-The\\_UK\\_as\\_a\\_world-leader\\_in\\_Safety\\_Tech.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-The_UK_as_a_world-leader_in_Safety_Tech.pdf) 25/05/2021
- 403 Safety by Design (Australian eSafety Commissioner, 2019) Accessed from: <https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Document8b.pdf> 25/05/2021
- 404 The Decentralised Web of Hate (Bevensee & Rebellious Data LLC, 2020) Accessed from: <https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf> 25/05/2021
- 405 What is a VPN? – Virtual Private Network (Cisco) Accessed from: [https://www.cisco.com/c/en\\_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html](https://www.cisco.com/c/en_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html) 25/05/2021
- 406 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: <https://www.netclean.com/2018/10/30/hash-values/> 25/05/2021
- 407 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: <https://www.netclean.com/2018/10/30/hash-values/> 25/05/2021
- 408 Use of AI in Online Content Moderation (Cambridge Consultants, 2019) Accessed from: [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf) 25/05/2021
- 409 Darknet Cybercrime Threats to Southeast Asia (UNODC, 2020) Accessed from: [https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet\\_Cybercrime\\_Threats\\_to\\_Southeast\\_Asia\\_report.pdf](https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf) 25/05/2021
- 410 End-to-End Encryption (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 25/05/2021
- 411 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 412 Metadata (WhatIs.com, 2021) Accessed from: <https://whatis.techtarget.com/definition/metadata> 24/06/2021
- 413 Tor (Investopedia, 2019) Accessed from: <https://www.investopedia.com/terms/t/tor.asp> 07/05/2021
- 414 Convention on the Rights of the Child (United Nations, 1989) Accessed from: <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> 25/05/2021
- 415 How we protect children's rights with the UN Convention on the Rights of the Child (UNICEF) Accessed from: <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> 25/05/2021
- 416 Explanatory Notes: General Comment no.25 on children's rights (5Rights Foundation, 2021) Accessed from: [https://5rightsfoundation.com/uploads/ExplanatoryNotes\\_UNCRGC25.pdf](https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRGC25.pdf) 25/05/2021
- 417 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WePROTECT Global Alliance, 2020) Accessed from: <https://www.weprotect.org/response/technology/> 25/05/2021
- 418 Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response (WePROTECT Global Alliance, 2016) Accessed from: <https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf> 25/05/2021
- 419 Lanzarote Convention (Council of Europe) Accessed from: <https://www.coe.int/en/web/children/lanzarote-convention> 25/05/2021
- 420 Glossary: E-privacy Directive 2009/136/EC (European Data Protection Supervisor) Accessed from: [https://edps.europa.eu/data-protection/data-protection/glossary/e\\_en#e-privacy-directive2009-136-ec](https://edps.europa.eu/data-protection/data-protection/glossary/e_en#e-privacy-directive2009-136-ec) 25/05/2021
- 421 The EU will continue to protect children from child sexual abuse online (European Commission, 2020) Accessed from: [https://ec.europa.eu/home-affairs/news/20200910\\_eu-continue-protect-children-from-child-sexual-abuse\\_en](https://ec.europa.eu/home-affairs/news/20200910_eu-continue-protect-children-from-child-sexual-abuse_en) 25/05/2021
- 422 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf>
- 423 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: [https://www.aic.gov.au/sites/default/files/2021-02/ti616\\_production\\_and\\_distribution\\_of\\_child\\_sexual\\_abuse\\_material\\_by\\_parental\\_figures.pdf](https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf) 28/05/2021



**WeProtect  
Global Alliance  
réunit des experts  
du gouvernement, du  
secteur privé et de la  
société civile.**

**Nous décomposons les  
problèmes complexes  
et développons des  
politiques et des  
solutions pour protéger  
les enfants contre les  
abus sexuels en ligne.**

