weprotect Global Alliance

CPC LEARNING NETWORK

COLUMBIA | MAILMAN SCHOOL OF PUBLIC HEALTH

Évaluation mondiale de la menace, 2025

Prévenir l'exploitation et les abus sexuels d'enfants facilités par la technologie : de l'analyse à l'action

Contents

Note sur le contenu et ressources

Ce rapport aborde l'exploitation et les abus sexuels d'enfants facilités par la technologie, et comprend des témoignages de survivants qui peuvent être bouleversants. Certains lecteurs pourraient trouver des sections du rapport difficiles à lire. Si ce contenu suscite une détresse ou des inquiétudes, veuillez consulter les ressources, disponibles mondialement et confidentielles listées ici.

Vous n'êtes pas seul(e) : vous pouvez obtenir de l'aide.

- Brave Movement, Get Help : plateforme regroupant les numéros d'assistance téléphonique nationaux.
- Child Helpline International : lignes d'assistance téléphonique pour enfants spécifiques à chaque pays.
- INHOPE : réseau mondial de lignes d'assistance téléphonique pour signaler le CSAM dans chaque pays.
- MOORE | Prévenir les abus sexuels sur les enfants, École de santé publique Johns Hopkins Bloomberg : conseils et ressources pour les personnes qui cherchent de l'aide pour elles-mêmes ou pour quelqu'un d'autre afin de prévenir les abus sexuels sur les enfants.
- ReDirection Self-Help Program : ressource en ligne confidentielle qui aide les personnes préoccupées par leurs pensées ou comportements sexuels envers les enfants.

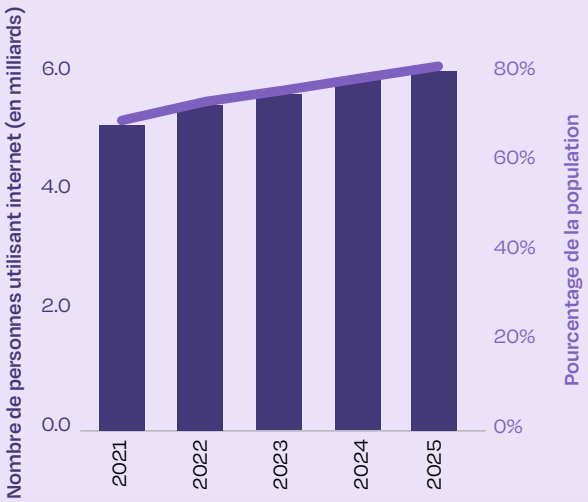
Résumé

> « L'avenir de notre monde numérique n'a pas à être effrayant, il peut être passionnant et enrichissant. Mais nous devons l'aborder avec prudence, responsabilité et transparence. À mesure que nous entrons dans cette nouvelle ère de l'Intelligence Artificielle, il nous faut veiller à ce que la jeune génération soit non seulement capable de naviguer dans ces espaces, mais aussi en mesure de les façonner pour en faire quelque chose de meilleur. »
>
> *Défenseur des jeunes*[1]

L'exploitation et les abus sexuels envers les enfants (désigné dans ce rapport par son acronyme anglais CSEA -Child Sexual Abuse and Exploitation) facilitée par la technologie constituent un défi mondial complexe qui cause un préjudice profond aux enfants, aux familles et aux communautés. Cette menace est **évitable, elle n'est pas une fatalité.**[2] Pour y faire face, il faut une action coordonnée et intersectorielle axée sur les droits des enfants. Des données et stratégies prometteuses apparaissent à l'échelle mondiale. Le Global Threat Assessment 2025 adopte une approche orientée vers l'action, évaluant le paysage actuel tout en mettant l'accent sur la prévention et les mesures concrètent pour protéger les enfants.

Le paysage numérique évolue rapidement, créant de nouvelles menaces pour les enfants et des défis en matière de détection et d'application de la loi. Plus de 6,0 milliards de personnes utilisent désormais Internet, et l'accès des jeunes dépasse celui de la population générale.[3,5] Plus de la moitié de la population mondiale possède désormais un smartphone.[4]

Figure 1 . Tendances de l'utilisation d'Internet au cours des cinq dernières années[5]



Si les technologies numériques offrent des possibilités inédites de connexion, d'apprentissage et d'expression, elles exposent également les enfants à de nouveaux risques. La technologie amplifie souvent les dangers, traversant les sphères physiques, sociaux et numériques. Les technologies existantes et émergentes, telles que l'intelligence artificielle générative (IA), le cryptage et la réalité étendue, remodèlent l'environnement numérique des enfants. En

quelques années seulement, l'IA générative, y compris les chatbots IA, est passée d'un stade largement expérimental à une intégration complète dans les réseaux sociaux, les plateformes de messagerie et les outils du quotidiens utilisés par les enfants.[6] Si ces évolutions offrent des avantages, elles créent également d'importants défis en matière de prévention, de détection et d'application de la loi. Les plateformes chiffrées renforcent la confidentialité des utilisateurs, mais peuvent également réduire les obstacles à la commission d'infractions contre les enfants. Elles rendent également plus difficile la détection, le blocage et la suppression du matériel d'abus sexuels d'enfant (désigné dans ce rapport par son acronyme anglais CSAM -*Child Sexual Abuse Material*). Les experts de la société civile soulignent une tendance persistante selon laquelle certains délinquants entrent en contact avec des enfants sur des plateformes ouvertes avant de déplacer leurs échanges vers des canaux chiffrés ou des environnements hors ligne dans l'intention de leur nuire. En outre, un nombre croissant d'éléments suggèrent que l'exploitation et les abus sexuels commis par des pairs sont en augmentation, et que l'exposition à des contenus sexuels inappropriés en ligne pourrait y contribuer.[7–9] Les préjudices causés par des pairs, des camarades de classe et des partenaires intimes surviennent souvent lorsque se conjuguent plusieurs facteurs, des mesures de protection numériques insuffisantes, une supervision défaillante et une éducation limitée sur les comportements appropriés en ligne et les comportements sexuels.[10,11]

La CSEA facilitée par la technologies continue de gagner en ampleur et en complexité, sous l'effet des changements technologiques rapides et des lacunes systémiques persistantes. Depuis 2023, les préjudices existants demeurent largement inchangés, tandis que de nouvelles menaces émergent plus vite que ne peuvent s'adapter les lois, les politiques et les mesures de protection. Les CSAM sont détectés, signalés et supprimés à des niveaux sans précédent. Les données fiables sur la prévalence mondiale demeurent insuffisantes, et il convient d'interpréter avec prudence les tendances observées dans les signalements, car celles-ci reflètent souvent les capacités et les pratiques en matière de signalement plutôt que l'ampleur réelle préjudices . Par exemple, les signalements à la **CyberTipline** du National Center for Missing and Exploited Children (NCMEC) sont passés de 36,2 millions en 2023 à 29,2 millions d'incidents, associés à 20,5 millions de signalements, en 2024. Cette diminution est largement attribuée aux pratiques de « regroupement », qui consistent à regrouper les signalements connexes, et au chiffrement de bout en bout, qui limite la détection et le signalement.[12]

INHOPE a reçu 2,5 millions de signalements de cas présumés de CSAM en 2024, soit plus du double de l'année précédente.[13]

Le NCMEC a reçu 20,5 millions de signalements de cas présumés d'exploitation sexuelle d'enfants en 2024.[12]

L'Internet Watch Foundation (IWF) a confirmé près de 300 000 cas de CSAM en 2024.[14]

L'IA générative a été utilisée pour faciliter la création et la distribution à massive de CSAM, dissimuler l'identité des victimes et des auteurs, et contourner les lois et les mesures de protection, telles que les méthodes de vérification de l'âge. Elle a également favorisé l'émergence de nouvelles formes d'abus sexuels sur mineurs, notamment l'extorsion sexuelle financière et les images « deepfake » représentant de vrais enfants dans des situations sexuelles simulées. Fin 2023, les premières images d'abus sexuels sur des enfants générées par l'IA ont été signalées via des lignes d'assistance téléphonique sur Internet et leur prévalence a depuis augmenté de manière exponentielle.[15] **La CyberTipline** du NCMEC a enregistré une augmentation de 1 325 % des signalements liés à l'IA générative entre 2023 et 2024, soit 67 000 signalements.[12] Ce volume met à rude épreuve les forces de l'ordre et les modérateurs de contenu.

Au cours des six premiers mois de 2025, plus de 440 000 signalements liés à l'IA générative et à l'exploitation sexuelle des enfants ont été reçus par le NCMEC.[12]

Le grooming et la séduction en ligne demeurent très répandus. En 2024, le NCMEC a enregistré 546 000 signalements, soit une augmentation de 192 % par rapport à 2023.[12] Les experts soulignent également les liens alarmants entre l'exploitation sexuelle des enfants facilitée par la technologie et d'autres préjudices, notamment les idées suicidaires et l'automutilation, l'extrémisme, la traite des êtres humains et les escroqueries à des fins financières. Ces phénomènes émergents nécessitent des recherches approfondies car ils restent mal compris. L'extorsion sexuelle financière est une tendance persistante qui touche de manière disproportionnée les garçons.

En 2024, le NCMEC a reçu environ 100 signalements d'extorsion sexuelle financière par jour.[12]

Une dynamique mondiale se renforce, visant à lutter contre l'exploitation sexuelle des enfants facilitée par la technologie.

Depuis 2023, plusieurs pays ont proposé ou adopté de nouvelles lois pour lutter contre ce problème. La **loi** américaine de 2024 sur **la sécurité en ligne (U.S. Report Act)** impose des obligations supplémentaires aux entreprises technologiques, notamment l'obligation de signaler au NCMEC les cas -auparavant volontaire, assorti d'amendes pouvant atteindre un million de dollars en cas d'infraction.[16] La loi britannique de 2023 sur **la sécurité en ligne (Online Safety Act)** étend de nouvelles exigences, notamment en matière d'évaluation des risques et de vérification de l'âge, à des centaines de milliers de fournisseurs de services en ligne dans le monde entier visant les utilisateurs britanniques.[17] Au Brésil, deux mesures historiques de protection de l'enfance ont été adoptées en 2025, notamment l'interdiction nationale de l'utilisation non éducative des smartphones dans les écoles et une nouvelle législation introduisant des obligations en matière de sécurité dès la conception et de signalement pour les plateformes en ligne.[19,20] L'Australie a adopté une limitation de l'âge d'accès aux réseaux sociaux (16 ans), qui est actuellement en cours de mise en œuvre.[18] À Singapour, l'autorité de régulation des télécommunications exigera bientôt un contrôle de l'âge pour télécharger certaines applications sur les appareils mobiles, une première mondiale.[21] L'impact total de cette vague de législations reste à déterminer, à mesure que ces politiques entrent dans leur phase de mise en œuvre. La **Convention des Nations unies contre la cybercriminalité**, adoptée en décembre 2024 et en voie de ratification, marque une étape importante dans la protection mondiale des enfants. Pour la première fois, elle fait du CSAM et du grooming en ligne des infractions au droit international.[22,23] Le **Pacte numérique mondial**, mis en œuvre en 2025, fournit un cadre pour la coopération internationale, guidant les efforts visant à lutter contre les préjudices en ligne et à renforcer la sécurité numérique.[24]

Des progrès notables ont également été réalisés grâce à l'adoption de la deuxième édition des **Lignes directrices terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels** (abrégées en Lignes directrices terminologiques), au lancement de partenariats intersectoriels innovants visant à améliorer la détection et la prévention, tels que **Lantern**, et à des études de recherche à grande échelle visant à combler les lacunes en matière de preuves.[25,26] **La revue systématique vivante** du Safe Futures Hub fournira des données actualisées, tandis que des initiatives telles que **Prevention Global** élargissent les connaissances sur la prévention des actes de violence et leur prévalence mondiale.[27,28]

Le point de vue des enfants reste sous-représenté. Malgré certaines approches prometteuses visant à intégrer le point de vue des enfants dans les politiques et la prise de décision, les enfants n'ont souvent pas la possibilité de participer de manière significative aux décisions politiques qui les concernent. Notre analyse de la littérature publiée depuis 2023 sur l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie a révélé qu'une minorité de publications incluaient la voix des enfants et que très peu les consultent pour obtenir des recommandations d'action. L'évaluation mondiale de la menace 2025 a donné lieu à des consultations avec des enfants afin d'éclairer et de façonner les recommandations présentées.

La CSEA facilitée par la technologie peut être prévenue, mais il n'existe pas de solution unique. La prévention nécessite une action de l'ensemble de la société. Le cadre de prévention présenté dans ce rapport, qui complète le modèle de réponse nationale de l'Alliance mondiale WeProtect, offre des conseils pratiques dans quatre domaines d'action interdépendants :[29]

- PARTICIPATION ET LEADERSHIP DES ENFANTS
- ÉDUCATION ET SOUTIEN COMMUNAUTAIRES
- SÉCURITÉ NUMÉRIQUE
- LOI, POLITIQUE ET JUSTICE

- Ces domaines d'action s'articulent autour de trois niveaux de prévention :
- primaire (protection proactive),
- secondaire (détection et prévention des dommages), et
- tertiaire (intervention et soutien après la survenue d'un dommage, ce qui peut empêcher la revictimisation et la récidive).

Le cadre synthétise les données émergentes, les bonnes pratiques et les recommandations d'experts. Il vise à fournir un point d'entrée permettant aux parties prenantes d'envisager des mesures de prévention adaptées à leur contexte et à leur expertise. Les domaines d'action sont organisés de manière à refléter le modèle socio-écologique, en commençant par les enfants pour englober les communautés, les institutions, les gouvernements et les acteurs mondiaux.[30] Ce modèle souligne la dimension imbriquée de la prévention, où chaque niveau renforce les autres. Les leviers essentiels, tels que le financement et la recherche, constituent le fondement de toutes les actions et doivent être abordés de manière proactive et soutenus pour rendre la prévention possible.

Cadre de prévention

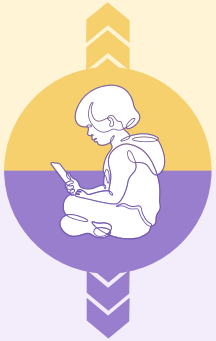
Principes Directeurs

Chaque enfant a le droit d'être protégé contre tout préjudice, y compris l'exploitation et les abus sexuels.
Les efforts visant à prévenir l'exploitation et les abus sexuels des enfants facilités par la technologie doivent :

- défendre les droits et la dignité des enfants et des survivants et éviter d'accroître les risques ou de causer davantage de préjudice ;
- reconnaître que les enfants sont à la fois exposés au risque d'être victimes de préjudices et d'adopter des comportements pouvant nuire à d'autres enfants ;
- être centrés sur les perspectives, les besoins et les préférences des enfants et des survivants ; et
- tenir compte des différences d'âge, de développement et d'autres caractéristiques des enfants, telles que l'identité de genre, l'orientation sexuelle, l'origine ethnique, le handicap, le statut de migrant, la situation économique et le niveau d'éducation, qui peuvent avoir une incidence sur leurs besoins et les risques auxquels ils sont exposés.

Facteurs favorisant l'exploitation et les abus sexuels des enfants facilités par la technologie

- Absence de mécanismes de protection
- Motivations financières
- Faiblesse de la gouvernance et de la responsabilité
- Vulnérabilités intersectionnelles
- Normes sociales néfastes



Facteurs favorables à la prévention

- Volonté politique
- Gouvernance numérique et responsabilité solides aux niveaux mondial, national et local
- Terminologie et systèmes de données harmonisés
- Coordination mondiale et intersectorielle
- Normes sociales favorables
- Professionnels et prestataires formés à l'accompagnement des enfants
- Systèmes de protection de l'enfance solides

Recherche et données

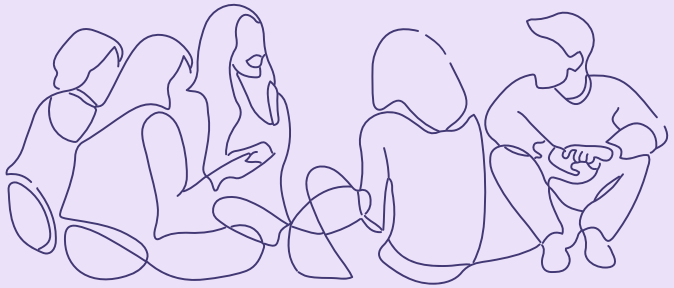
- Utiliser une approche de santé publique pour définir le problème et sa prévalence, identifier les facteurs de risque et de protection, concevoir et tester des interventions, et développer celles qui fonctionnent.
- Donner la priorité à la recherche informée ou menée par les enfants, les jeunes, les survivants et les populations marginalisées
- Approfondir les connaissances et les bonnes pratiques dans les pays à revenu faible et intermédiaire et dans les contextes sous-représentés
- Partager les données, les connaissances et les bonnes pratiques entre les régions et les secteurs, en adaptant les preuves avec sensibilité aux nouveaux contextes
- Réaliser des analyses coûts-avantages pour renforcer les arguments en faveur du financement de la prévention

Financement durable

- Lignes budgétaires dédiées dans les stratégies nationales
- Engagements de l'industrie
- Participation des institutions multilatérales
- Mécanismes de financement flexibles
- Financement intersectoriel
- Soutien durable aux organisations communautaires
- Financement de l'innovation et de la production de résultats scientifiques

PARTICIPATION ET LEADERSHIP DES ENFANTS

Impliquer de manière significative les enfants dans la définition des problèmes et l'élaboration des politiques, programmes et services qui les concernent.



Prévention primaire **PROTÉGER DE FAÇON PROACTIVE**	Prévention secondaire **DÉTECTER ET METTRE UN TERME AUX PRÉJUDICES**	Prévention tertiaire **SOUTENIR ET RÉAGIR**
Concevez avec les enfants des initiatives d'éducation et de sensibilisation adaptées au contexte, qui reflètent la manière dont ils utilisent la technologie, les personnes en qui ils ont confiance et les personnes vers lesquelles ils se tournent pour obtenir de l'aide s'ils sont victimes de préjudices ou s'ils ont des inquiétudes concernant leurs propres pensées et comportements.	Collaborez avec des organisations dirigées par des enfants et des survivants pour concevoir, mettre en œuvre et évaluer conjointement des canaux de signalement accessibles, faciles à utiliser et fiables, y compris des canaux non formels, tels que des pairs formés.	Utiliser les éclairages et les données fournies par les enfants et les adultes survivants pour améliorer l'accessibilité et la qualité des services d'aide, des systèmes judiciaires et des mécanismes de réparation. Explorer les concepts propres aux survivants en matière de préjudice, de justice et de responsabilité, y compris les approches non formelles et de justice réparatrice.

Ne consultez les enfants que lorsque du personnel formé, des mesures de sécurité et des services de soutien sont en place. Sinon, consultez les jeunes et les adultes qui peuvent représenter le point de vue des enfants, y compris les adultes survivants.

Créer des espaces sûrs et accueillants, tant en ligne que hors ligne, où les enfants peuvent partager leurs points de vue et influencer les politiques, les programmes et les services.

Impliquer des enfants de tous âges, sexes et origines, et éliminer les obstacles à l'inclusion. Solliciter l'avis des enfants qui ont subi des préjudices, ainsi que celui des enfants qui ont causé des préjudices.

ÉDUCATION ET SOUTIEN COMMUNAUTAIRES

Doter les enfants, les personnes qui s'occupent d'eux et les communautés des connaissances, des compétences et des outils nécessaires pour assurer la sécurité des enfants et réagir de manière appropriée aux risques et aux préjudices. Intervenir rapidement auprès des enfants et des adultes susceptibles de causer des préjudices.

Prévention primaire **PROTÉGER DE FAÇON PROACTIVE**	Prévention secondaire **DÉTECTER ET METTRE UN TERME AUX PRÉJUDICES**	Prévention tertiaire **SOUTENIR ET RÉAGIR**
Mettre en œuvre et évaluer des initiatives d'éducation et de sensibilisation fondées sur des résultats scientifiques qui favorisent la sécurité numérique, le signalement et la recherche d'aide. Veiller à ce qu'elles soient accessibles, disponibles en plusieurs langues et diffusées dans les écoles, les communautés et sur les plateformes numériques utilisées par les enfants. Apprendre aux enfants comment assurer leur sécurité et celle des autres en ligne et hors ligne, où trouver de l'aide, vers quels adultes de confiance se tourner pour obtenir de l'aide et comment signaler leurs préoccupations concernant certains comportements, leur propre sécurité ou celle d'autrui.	Mettre en place plusieurs canaux de signalement formels et informels, accessibles et adaptés aux enfants, notamment des lignes d'assistance téléphonique, des pairs formés et des adultes de confiance qui peuvent fournir un soutien et des ressources dès les premiers signes. Former les pairs, les aidants, les éducateurs et les prestataires de services à aider les enfants à rester en sécurité en ligne et hors ligne, et à réagir de manière appropriée aux préoccupations ou aux signalements de préjudice. Mettre en place des interventions précoces fondées sur des données pour les enfants et les adultes qui risquent de causer ou de subir des préjudices.	Soutenir les survivants et veiller à ce qu'ils connaissent leurs droits, les options qui s'offrent à eux, les services disponibles et les mesures qu'ils peuvent prendre pour se protéger contre d'autres préjudices, demander la suppression d'images et obtenir justice. Fournir des services adaptés aux traumatismes et centrés sur les survivants, tant pour les enfants que pour les adultes. Ces services doivent traiter les préjudices en ligne et hors ligne, favoriser la sécurité et la dignité et prévenir d'autres préjudices. Ils doivent inclure une assistance juridique, sanitaire, psychologique et psychosociale. Fournir des réponses fondées sur des données et non carcérales aux enfants qui ont causé des dommages afin de les réhabiliter et de prévenir la récidive.

SÉCURITÉ NUMÉRIQUE

Protéger les enfants en donnant la priorité à leur sécurité, leur bien-être et leurs droits dans la culture industrielle et dans la conception et le développement des produits, services et infrastructures numériques.

Prévention primaire **PROTÉGER DE FAÇON PROACTIVE**	Prévention secondaire **DÉTECTER ET METTRE UN TERME AUX PRÉJUDICES**	Prévention tertiaire **SOUTENIR ET RÉAGIR**
Donner la priorité à la sécurité, aux droits et au bien-être des enfants à tous les niveaux de la culture d'entreprise, de la prise de décision et de la formation du personnel. Faire de la sécurité dès la conception la norme, en intégrant des évaluations d'impact sur les droits des enfants et des examens de risques rigoureux dans les processus de développement. Consulter les enfants et les jeunes pour éclairer les choix de conception et veiller à ce que les dispositifs de sécurité soient fonctionnels, accessibles et disponibles de manière équitable dans tous les lieux et toutes les langues où un produit ou un service est proposé. Harmoniser la terminologie et les indicateurs de transparence afin d'améliorer la comparabilité entre les produits et services.	Détecter et interrompre les contenus et les comportements préjudiciables à l'aide d'outils en temps réel qui respectent la vie privée et les droits des utilisateurs (par exemple, correspondance de hachage, fenêtres contextuelles d'avertissement, redirection vers des services d'assistance, détection des comportements de grooming et des transactions financières à risque). Financer et fournir un soutien psychosocial et en matière de santé mentale aux intervenants de première ligne dans le domaine numérique.	Fournir des canaux de signalement accessibles et adaptés aux enfants au sein des plateformes. Ceux-ci doivent mettre les utilisateurs en relation directe avec des lignes d'assistance et des services d'aide, et fournir des réponses rapides. Garantir des processus sûrs et sans stigmatisation permettant aux victimes de demander le retrait de leurs images. Renforcer la transparence et la prise de responsabilité en rendant publique les informations disponibles sur l'impact des produits et services numériques sur les droits des enfants dans tous les pays où ils sont disponibles. Collecter et partager des données anonymisées et désagrégées sur la sécurité afin de renforcer l'apprentissage à l'échelle du secteur et entre les secteurs. Collaborer à l'échelle du secteur pour supprimer le CSAM et autres contenus préjudiciables.

LOI, POLITIQUE ET JUSTICE

Renforcer les systèmes juridiques et réglementaires afin de prévenir les abus, garantir la justice et tenir les responsables pour redevables.

Prévention primaire **PROTÉGER DE FAÇON PROACTIVE**	Prévention secondaire **DÉTECTER ET METTRE UN TERME AUX PRÉJUDICES**	Prévention tertiaire **SOUTENIR ET RÉAGIR**
Renforcer, harmoniser et appliquer les lois et réglementations en utilisant une terminologie universelle et en définissant clairement les obligations et les sanctions. Consulter les survivants, les groupes de défense des droits des enfants, l'industrie et les autres parties prenantes afin d'aligner la législation sur les lois relatives aux droits des enfants, les résultats scientifiques et les bonnes pratiques, et de permettre une innovation responsable dans l'industrie. Concevoir des lois qui reconnaissent les différences de développement entre les enfants et les adultes, mettent l'accent sur la réadaptation des enfants qui causent du tort et évitent de criminaliser les comportements mutuellement consentis entre pairs d'âge proche. Mettre en place des organismes de réglementation nationaux/régionaux dotés des pouvoirs, des ressources et de l'expertise technique nécessaires pour établir des normes, contrôler leur respect et garantir une surveillance et une véritable responsabilité de l'industrie.	Mettre en place des systèmes proactifs pour détecter, enquêter et réagir aux cas d'abus sexuels commis sur des enfants à l'aide de technologies, plutôt que de se fier uniquement aux signalements des victimes. Exiger des institutions financières qu'elles détectent et signalent activement les transactions liées à l'exploitation sexuelle des enfants. Mettre en place des canaux de signalement accessibles, adaptés aux enfants et tenant compte des traumatismes, reliés à des services d'aide, et fournir des informations claires sur les endroits où les personnes peuvent signaler des cas ou demander de l'aide dans leur pays.	Former les forces de l'ordre, les magistrats et les procureurs à des procédures adaptées aux enfants, tenant compte des traumatismes subis et centrées sur les survivants, qui respectent les droits, la dignité et l'intérêt supérieur des enfants. Mettre en place des bases de données nationales anonymisées sur les victimes afin d'informer les mesures de prévention et d'intervention. Utiliser un suivi et une réadaptation fondés sur des données scientifiques pour prévenir la récidive. Traiter les enfants en conflit avec la loi conformément aux normes internationales en matière de justice pour mineurs. Recourir à la réadaptation, à la déjudiciarisation et aux peines alternatives. Éviter la détention, l'enregistrement et la notification.

Recommandations

Les recommandations issues de l'évaluation mondiale des menaces 2025 soulignent la nécessité d'une action mondiale coordonnée pour prévenir l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie. Ensemble, elles décrivent une approche globale et multisectorielle visant à protéger les enfants tant en ligne que hors ligne.

Recommandations transversales à l'intention de toutes les parties prenantes

1. **Traiter la CSEA facilitée par la technologie comme une priorité urgente de santé publique et investir dans des stratégies de prévention, notamment celles visant à prévenir les actes de CSEA et à réduire la stigmatisation associée à la recherche d'aide et à la divulgation.** Reconnaître que les enfants sont à la fois exposés au risque d'être victimes et à celui d'adopter des comportements préjudiciables envers d'autres enfants.

2. **Produire et utiliser des données probantes pour éclairer la prévention.** Impliquer de manière sûre et éthique les enfants et les survivants afin de définir le problème et d'identifier les obstacles à l'inclusion des populations marginalisées.

3. **Collaborer entre les secteurs pour coordonner les efforts de prévention et partager les enseignements.** Adopter une terminologie harmonisée conforme aux lignes directrices terminologiques, normaliser les indicateurs/systèmes de signalement, partager en temps utile les données et les preuves de ce qui fonctionne et de ce qui ne fonctionne pas, et mettre en place des systèmes durables.[26]

Organisations de la société civile, y compris les ONG internationales

1. **Créer des espaces sûrs et inclusifs où les enfants et les survivants peuvent partager leurs points de vue et influencer les efforts de prévention et de plaidoyer.** S'efforcer d'impliquer les enfants marginalisés, notamment les enfants handicapés, les minorités sexuelles et de genre, les enfants ruraux et non scolarisés, les enfants issus de minorités ethniques ou de milieux migrants, et les enfants qui n'ont pas accès aux technologies numériques.

2. **Plaider pour des mesures de prévention et de réponse fondées sur les droits ainsi que de mécanismes robustes d'obligation de rendre des comptes, pour lutter contre la CSEA facilitée par la technologie.**

3. **Renforcer les services communautaires de signalement et de soutien, notamment les lignes d'assistance téléphonique et les réseaux de pairs.** Former les personnes qui s'occupent d'enfants, les éducateurs et les prestataires de services à fournir un soutien précoce et sans jugement et à orienter vers des ressources ; proposer des services accessibles, centrés sur les survivants, pour enfant et adulte, qui traitent à la fois les préjudices en ligne et hors ligne, favorisent le bien-être à long terme et préviennent la revictimisation.

4. **Mettre en place des interventions précoces fondées sur des données probantes pour les enfants et les adultes qui risquent de causer ou de subir des préjudices,** et apporter des réponses probantes non carcérales pour les enfants qui ont causé des préjudices.

Secteur privé, en particulier les entreprises technologiques

1. **Donner la priorité à la sécurité, aux droits et au bien-être des enfants à tous les niveaux et notamment dans la culture d'entreprise, la prise de décision et la formation du personnel.** Offrir une formation continue tout au long du processus de recrutement, investir dans la recherche en matière de prévention et dans les services d'aide aux survivants, et veiller à ce que les intervenants numériques de première ligne et les équipes chargées de la sécurité numérique (équipes « Confiance et Sécurité ») bénéficient d'un soutien et de ressources suffisants.

2. **Faire de la sécurité dès la conception la norme, en intégrant les évaluations d'impact sur les droits des enfants et la diligence raisonnable dans les processus de développement.** Consulter en toute sécurité les enfants , les jeunes et les survivants afin d'éclairer les choix de conception. Veiller à ce que les dispositifs de sécurité soient fonctionnels, accessibles et disponibles de manière équitable dans toutes les régions géographiques et toutes les langues où un produit ou un service est proposé.

3. **Renforcer la transparence et redevabilité.** Publier tous les impacts significatifs sur les droits de l'enfant des produits et services numériques par le biais des cadres de signalement existants dans chaque pays d'activité.[31] Collecter et partager des données de sécurité anonymisées et désagrégées avec les chercheurs, les régulateurs et tous les secteurs afin d'éclairer la prévention. Intégrer des mécanismes de indépendants de redevabilité au sein de la gouvernance d'entreprise.

4. **Détecter et contrer de manière proactive les contenus et les comportements préjudiciables.** Utiliser des outils en temps réel respectueux des droits, tels que la correspondance d'empreinte(hashage), la surveillance, les fenêtres contextuelles d'avertissement, la redirection vers des services d'assistance ainsi que la détection des comportements de sollicitations -ou grooming et des transactions financières à risque. Parallèlement, fournir des canaux de signalement adaptés aux enfants et accessibles qui relient directement les utilisateurs à des lignes d'assistance et à des services de soutien, supprimer rapidement les contenus préjudiciables et répondre en temps utile aux signalements.

Milieu universitaire et chercheurs

1. **Donner la priorité à la recherche sur la prévalence, les facteurs de risque et de protection, et les facteurs systémiques de la CSEA facilitée par la technologie.** Combler les lacunes critiques en matière de recherche, notamment les vulnérabilités intersectionnelles, l'escalade en ligne-hors ligne, et les stratégies efficaces de prévention des actes criminels, y compris la lutte contre l'apparition de comportements sexuels préjudiciables chez les enfants et les jeunes.

2. **Concevoir, adapter et évaluer des interventions dans différents contextes et auprès de différentes populations. Établir des partenariats intersectoriels et mener des recherches sur la rentabilité et la mise en œuvre afin d>orienter les investissements durables.**

3. Établir des partenariats de recherche conjoints, coordonner les programmes de recherche et promouvoir le partage rapide des données.

Gouvernements

1. **Réviser, renforcer et harmoniser les lois et réglementations mondiales afin de lutter contre la CSEA facilitée par la technologie.** Consulter largement les parties prenantes afin d'aligner la législation sur les données probantes, les bonnes pratiques et les lois et normes relatives aux droits de l'enfant. Utiliser une terminologie harmonisée et veiller à ce que la législation soit neutre sur le plan technologique, couvrant à la fois les technologies existantes et futures. Définir des obligations, des sanctions et des mécanismes de responsabilité clairs pour les responsables, tout en permettant une innovation responsable dans le secteur. Faire la distinction

entre les comportements des adultes et ceux des adolescents et éviter de criminaliser les comportements mutuellement consentis entre pairs d'âge similaire.

2. **Mobiliser et coordonner les systèmes nationaux de protection de l'enfance et de justice afin de lutter contre les préjudices causés aux enfants tant en ligne que hors ligne.** Mettre en place plusieurs canaux de signalement accessibles, adaptés aux enfants et tenant compte des traumatismes, reliés à des services de santé, psychosociaux et juridiques complets. Tenir à jour des bases de données sécurisées et anonymisées sur les victimes afin d'orienter la prévention et les mesures d'intervention. Former les forces de l'ordre, les magistrats, les éducateurs et les travailleurs de première ligne à des pratiques adaptées aux enfants et tenant compte des traumatismes, et leur apporter un soutien continu pour leur bien-être.
3. **Utiliser un suivi et une réinsertion fondés sur des données probantes pour prévenir la récidive et donner la priorité au soutien, à la déjudiciarisation et aux peines alternatives pour les enfants en conflit avec la loi.**
4. **Mettre en place des organismes de réglementation nationaux ou régionaux indépendants dotés de l'autorité, des ressources et de l'expertise technique nécessaires pour lutter contre l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie,** notamment en établissant des normes, en contrôlant leur respect et en appliquant des sanctions.
5. **Mettre en œuvre et évaluer des programmes nationaux d'éducation et de sensibilisation fondés sur des données probantes qui visent à promouvoir la sécurité numérique, le signalement et la recherche d'aide.** Intégrer une éducation adaptée à l'âge dans les programmes scolaires et former les enseignants, les personnes qui s'occupent des enfants et les prestataires de services. Mener des campagnes d'éducation et de sensibilisation accessibles et multilingues, en collaboration avec les communautés et d'autres secteurs afin d'atteindre les enfants marginalisés.

Organisations intergouvernementales

1. Faciliter la coopération transfrontalière en matière d'application de la loi et le partage de renseignements.
2. **Fournir une assistance technique et mobiliser des ressources pour renforcer les capacités nationales**, en établissant des priorités en fonction des besoins et de la prévalence.
3. **Mobiliser des financements communs et durables** pour soutenir les gouvernements nationaux, les organisations communautaires et les initiatives de prévention innovantes.

Avant-propos

« Mes images sont vendues en ligne depuis plus de 20 ans. Je suis victime de CSAM chaque jour de ma vie. J'ai été abusé quand j'étais enfant, lorsque mon premier agresseur a créé mon CSAM. Depuis lors, chaque semaine, mes avocats reçoivent de nouvelles notifications indiquant que « mon » matériel a été trouvé dans la collection d'un autre pédophile. Il y a plus de dix ans, j'ai saisi la Cour suprême des États-Unis avec mes avocats du cabinet Marsh Law.

Ma série de CSAM est si populaire que je sais que sa diffusion ne cessera jamais. Mais toutes les victimes de CSAM ne doivent pas nécessairement subir le même sort. La technologie permettant d'intervenir, de détecter et d'arrêter la propagation du CSAM existe. Nous devons obliger les grandes entreprises technologiques à l'utiliser.

J'étais adolescent lorsque j'ai découvert que mes CSAM étaient échangés dans le monde entier. À l'époque, j'étais l'une des rares victimes de ce crime odieux. Aujourd'hui, il y a... [Des centaines de millions d'] enfants victimes chaque année.

Aujourd'hui, j'élève un adolescent dans un monde qui devient chaque jour plus dangereux. Il est extrêmement difficile d'élever des jeunes enfants à l'ère de la technologie toxique. Comment puis-je m'assurer que mes enfants ne tomberont jamais sur mon CSAM alors qu'il est littéralement partout sur Internet ? Comment puis-je protéger mes enfants des prédateurs alors que je sais qu'ils ne sont qu'à deux clics du danger ?

Je suis extrêmement fière de voir des victimes comme moi, et des parents comme moi, s'attaquer aux grandes entreprises technologiques. Mais soyons clairs : pour avoir une chance de réussir, nous aurons besoin de recherches innovantes, d'outils de pointe pour faire respecter la loi et du soutien sans faille de défenseurs dévoués. Je ne sais pas comment nous allons y parvenir, mais je sais que nous devons à tous les enfants de ne pas abandonner.

Je n'ai pas de réponse à la question de savoir comment protéger les enfants en ligne de nos jours, mais je sais une chose : WeProtect [Global Alliance] a été une bouée de sauvetage pour les survivants dans cette lutte pour la vie de nos enfants. Grâce à ce réseau de soutien, je vois enfin la lumière au bout du tunnel. Les problèmes liés au CSAM en ligne s'aggravent chaque jour et le manque de responsabilité s'accentue. Mais les écoles interdisent les téléphones, les entreprises technologiques prennent conscience du problème, la vérification de l'âge se généralise, les systèmes de soutien se développent et les survivants partout dans le monde osent parler.

Nous avançons enfin dans la bonne direction. »

Cette déclaration a été fournie, avec le soutien de Protect Children, par un survivant qui, comme beaucoup d'autres, a choisi de rester anonyme. WeProtect Global Alliance a invité ce contributeur anonyme à partager son témoignage aux côtés de nombreuses autres personnes ayant vécu des expériences similaires, qu'il s'agisse d'enfants que nous cherchons à protéger dans le monde numérique ou de survivants d'abus sexuels facilités par la technologie, car ces voix sont trop souvent ignorées. Dans cette évaluation mondiale des menaces, nous intégrons ces expériences vécues dans les preuves et les recherches, en fondant notre travail sur la réalité des personnes. Nous reconnaissons que ces voix sont complexes, diverses et parfois en désaccord, mais elles doivent être entendues.

Introduction

Objectifs

L'exploitation et les abus sexuels des enfants -désigné par l'abréviation anglaise CSEA dans ce rappport (*Child Sexual Exploitation and Abuse*) facilités par la technologie, constituent un défi mondial complexe qui porte gravement atteinte aux enfants, aux familles et aux sociétés. La prévention et la lutte contre ces préjudices nécessitent une action urgente et coordonnée entre les secteurs et au-delà des frontières.

L'évaluation mondiale des menaces 2025 a deux objectifs :

1. Analyser les tendances mondiales en matière de CSEA facilitée par la technologie depuis 2023.
2. Concevoir conjointement un cadre de prévention avec des experts, des défenseurs des jeunes et des survivants, en fournissant des recommandations concrètes alignées sur le modèle de réponse nationale de l'Alliance mondiale WeProtect.

L'évaluation mondiale de la menace 2025 souligne la nécessité d'adopter des approches adaptées au contexte. Les risques encourus par les enfants, leur accès aux technologies numériques et aux ressources de protection, ainsi que la solidité des systèmes de protection varient considérablement d'une région à l'autre. Le rapport révèle d'importantes lacunes en matière de protection et souligne le besoin urgent d'équité dans les efforts de prévention mondiaux, en particulier pour protéger les enfants dans les environnements sous-réglementés ou disposant de ressources limitées.

Un cadre fondé sur les droits de l'enfant

> « Les jeunes devraient avoir le droit de comprendre leurs droits en ligne. La reconnaissance de ces droits constituerait déjà un pas en avant pour leur permettre de se sortir de situations dangereuses. »

Jeune fille de 14 ans, Canada[32]

La prévention de la CSEA facilitée par la technologie est un impératif juridique et éthique fondé sur le droit international des droits de l'homme. La Convention des Nations Unies relative aux droits de l'enfant exige des États qu'ils protègent les enfants contre toutes les formes de violence, d'exploitation et d'abus. L'observation générale n° 25 confirme que ces droits s'étendent aux espaces numériques et exige des gouvernements qu'ils intègrent les droits des enfants dans leur politique numérique, garantissent l'accès à la justice et consultent les enfants sur les décisions qui les concernent.[33,34] Alors que la Convention relative aux droits de l'enfant établit les obligations des États en tant que responsables, les principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme et les principes relatifs aux droits de l'enfant et aux entreprises définissent la responsabilité du secteur privé de respecter les droits des enfants, de prévenir les violations de ces droits et d'y répondre.[35,36] Ces principes sous-tendent l'analyse des tendances mondiales présentée dans le présent rapport et éclairent le cadre de prévention et les recommandations qui suivent.

Remarque sur la terminologie

En 2025, un groupe de travail inter-institutions mondial a mis à jour les lignes directrices de Luxembourg et publié la deuxième édition des **lignes directrices terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels** (abrégées en « lignes directrices terminologiques »).[28] Conformément à ces lignes directrices, le présent rapport utilise le terme « exploitation et abus sexuels d'enfants (CSEA) facilitée par la technologie». La **CSEA facilitée par la technologie** désigne l'utilisation des technologies numériques à n'importe quel stade pour préparer, commettre ou diffuser (dans le cas du matériel d'abus sexuels d'enfants, ou CSAM) l'exploitation sexuelle ou les abus sexuels d'un enfant. Elle englobe les préjudices commis dans des environnements numériques et non numériques (hors ligne), y compris, par exemple, l'échange d'informations, la coordination d'actions et la prise de contact avec des enfants dans le but de les manipuler ou de les contraindre. Ce terme reconnaît que la technologie joue un rôle dans la facilitation des abus et la perpétuation des dommages causés par ces derniers, tant dans les espaces physiques que numériques.

Un **enfant** désigne toute personne âgée de moins de 18 ans. Les enfants, y compris les adolescents, diffèrent en fonction de caractéristiques telles que l'âge, le stade de développement, l'orientation sexuelle, l'identité de genre, le handicap, l'origine ethnique, le niveau d'éducation, la situation économique et le statut migratoire. Ces facteurs interdépendants peuvent avoir une incidence sur les risques et les préjudices auxquels les enfants sont exposés, ainsi que sur leur accès aux ressources de protection. Un **survivant** est une personne qui a été victime d'exploitation ou d'abus sexuels. De nombreux survivants de CSEA facilitée par la technologie sont aujourd'hui des adultes qui devraient également être inclus dans les efforts de prévention et d'intervention. En reconnaissant que les personnes ayant vécu cette expérience utilisent différents termes pour se décrire, le présent rapport utilise indifféremment les termes « **victime** » et « **survivant** ».

Méthodologie

Ce rapport s'appuie sur un large éventail de sources de données et d'expertises. Il a été guidé par un comité directeur d'experts composé de 14 représentants du gouvernement, des forces de l'ordre, du secteur privé, de la société civile, du monde universitaire, d'organisations internationales et de défenseurs ayant vécu cette expérience.

Les données ont été synthétisées à partir de :

- Une revue exploratoire de la littérature universitaire et grise liée aux deux objectifs du rapport, publiée en anglais entre janvier 2023 et octobre 2025.
- Des entretiens semi-structurés avec 32 parties prenantes de différents secteurs et régions, menés de juin à juillet 2025, afin de recouper les points de vue et de combler les lacunes de la littérature.
- Une enquête en ligne menée auprès de 77 experts en septembre 2025 afin de recueillir des points de vue multisectoriels sur la hiérarchisation des mesures de prévention.
- Les conclusions de quatre ateliers réunissant des jeunes et des survivants, animés par des organisations spécialisées. Les survivants ont également examiné les guides d'entretien et de groupe de discussion afin d'en garantir la pertinence et la sensibilité.
- Études de cas partagées par des organisations et des membres de l'Alliance mondiale WeProtect, présentant des pratiques prometteuses et des réponses innovantes.

La diversité géographique a été assurée par la sélection des parties prenantes, des exemples de bonnes pratiques et des études de cas, en accordant une attention particulière aux régions et aux contextes sous-représentés. Le cadre de prévention a été co-créé et examiné dans le cadre de processus participatifs qui s'appuyaient sur cette diversité et cette représentation.

Parmi les limites, on peut citer la restriction aux publications en anglais, qui limite la représentation régionale, le délai court pour la collecte des données et le biais de sélection potentiel dans l'inclusion des parties prenantes et des études de cas, malgré les efforts déployés pour garantir la diversité géographique et sectorielle.

Le Manifeste SafetyNet : la voix des jeunes pour un avenir numérique plus sûr

Afin de mieux comprendre comment les enfants et les jeunes vivent le monde numérique et imaginent un avenir en ligne plus sûr, WeProtect Global Alliance a mené la deuxième phase du projet #MyVoice#MyFuture. Grâce à des consultations menées auprès de 109 jeunes âgés de 13 à 24 ans dans 10 pays, et en collaboration avec sept organisations de jeunesse, l'initiative a recueilli des informations sur la sécurité numérique, les droits et la CSEA facilitée par la technologie. Le résultat est le **Manifeste SafetyNet**, une déclaration des droits numériques rédigée par des jeunes et une feuille de route pour construire un avenir numérique plus sûr et plus équitable. Le Manifeste appelle à des protections plus fortes, à une conception inclusive et à une action collective afin de garantir que tous les enfants et les jeunes puissent exister en ligne sans crainte.[37]

Figure 2. Manifeste SafetyNet publié sur le Safe Futures Hub en juin 2025[38]

Le paysage numérique

Les enfants d'aujourd'hui grandissent à une époque de transformation numérique rapide. Si l'environnement numérique offre de précieuses opportunités d'apprentissage, de connexion, d'expression et d'appartenance, il peut également exposer les enfants à des risques et des dangers importants, tant en ligne que hors ligne. Ces opportunités et ces risques ont évolué rapidement ces dernières années, accélérés par l'essor de technologies telles que l'intelligence artificielle générative (IA), les environnements de réalité étendue (XR), la décentralisation, l'informatique quantique et le chiffrement de bout en bout, qui ont remis en question la capacité à prévenir, détecter et répondre à la CSEA facilitée par la technologie.[39]

Les enfants sont plus connectés que jamais, mais les inégalités numériques persistent.[40] On compte aujourd'hui 6,0 milliards d'internautes, soit environ les trois quarts de la population mondiale, contre 64 % en 2021.[5] Plus de la moitié de la population mondiale possède désormais un smartphone.[4] Dans certains pays de la majorité mondiale, la plupart du trafic web se fait sur des appareils mobiles, qui sont souvent partagés au sein des foyers ou entre amis.[41] Par exemple, 88 % du trafic web aux Philippines et 85 % au Nigeria provenaient d'un appareil mobile en février 2025.[41]

L'utilisation d'Internet par les jeunes dépasse celle du reste de la population de 13 %.[42] Une enquête mondiale menée auprès de plus de 380 000 enfants dans 55 pays a révélé que la majorité d'entre eux ont commencé à utiliser un appareil numérique avant l'âge de 10 ans.[43] En quelques années seulement, les technologies d'intelligence artificielle sont passées d'un stade largement expérimental à une intégration complète dans les réseaux sociaux, les plateformes de messagerie et les outils quotidiens utilisés par les enfants, tels que les agents conversationnels (chatbots) fondés sur l'IA.[6,44] Si l'IA offre des avantages éducatifs et sociaux, elle amplifie rapidement les risques et les dangers pour les enfants, notamment l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie. Les efforts visant à exploiter son potentiel pour protéger les enfants accusent un retard. Les résultats de **l'indice de bien-être numérique** 2025 (Digital Well-Being Index 2025) révèlent que 80 % des adolescents et des jeunes adultes de la génération Z déclarent avoir été exposés à une forme de risque en ligne.[45] Les interactions potentiellement liées à la sollicitation à des fins d'exploitation et d'abus sexuels, ainsi que le partage d'images intimes, étaient fréquentes. Environ un répondant sur quatre a indiqué avoir été exposé à des images sexuelles générées par IA, tandis que 25 % des participants ignoraient que la participation à la création ou au partage d'images à caractère sexuel impliquant des mineurs est illégale.[45]

Si de plus en plus d'enfants dans le monde ont accès aux technologies numériques, cet accès – et avec lui, l'exposition aux risques – reste inégal. Près de la moitié des six millions d'écoles dans le monde n'ont pas accès à Internet, la plupart d'entre elles se trouvant dans les pays de la majorité mondiale et dans les zones rurales reculées.[46] Un statut socio-économique élevé est systématiquement associé à une meilleure maîtrise du numérique, et la fracture numérique agit comme « un amplificateur d'exclusions sociales plus larges ».[47] Les enfants qui n'ont pas accès à des appareils numériques restent exposés à des risques, car les abus sexuels en personne sont souvent enregistrés, stockés et diffusés via les technologies numériques, y compris les appareils partagés.

Paysage juridique et politique

Ces dernières années, les gouvernements et les organismes internationaux ont fait progresser les réponses législatives et politiques, en cherchant à harmoniser les lois, à renforcer la réglementation et à s'adapter à l'évolution rapide des technologies. **La Convention des Nations unies contre la cybercriminalité** (2024) établit la première norme universelle contre la cybercriminalité, couvrant explicitement les crimes contre les enfants tels que la CSAM et la sollicitation des enfants en ligne (grooming), tout en renforçant le partage international des preuves.[23] La **première Conférence ministérielle mondiale sur l'élimination de la violence à l'encontre des enfants** (2024) a catalysé la coordination multisectorielle et les engagements nationaux visant à renforcer les cadres de protection de l'enfance, notamment en matière de préjudices en ligne.[48]

La version 3 du schéma de classification universel (Universal Classification Schema Version 3 - 2025) fournit un cadre harmonisé pour identifier, catégoriser et lutter contre la diffusion et la circulation de CSAM, avec des libellés lisibles par machine et des définitions harmonisées à l'échelle mondiale.[49] La deuxième édition des **lignes directrices terminologiques** (2025) fournit une base terminologique universelle pour faciliter la réforme juridique.[26] Une « troisième vague » de réformes législatives a vu le jour dans plusieurs pays, caractérisée par une meilleure harmonisation, notamment en matière de restrictions d'âge sur les réseaux sociaux, l'adaptation aux technologies futures (future-proofing) et et les efforts pour combler les lacunes juridiques concernant les nouvelles formes de préjudice, telles que les images d'abus sexuels sur enfants générées par IA et l'extorsion sexuelle.[50] Cependant, de nombreux cadres de protection de l'enfance restent fragmentés ou obsolètes, avec des autorités de régulation aux mandats incohérents et des protections limitées contre les contenus sexuels autoproduits impliquant des enfants ou les abus facilités par l'IA.[50,51] Dans certains contextes, les enfants victimes d'extorsion sexuelle risquent toujours d'être criminalisés, ce qui reflète les écarts entre la loi, les politiques et la réalité vécue par les enfants.[52]

Les difficultés persistantes en matière d'application de la loi et de réglementation continuent de compromettre les progrès. Les enquêtes transfrontalières sont ralenties par la fragmentation des juridictions, l'inégalité des ressources et la faiblesse des systèmes de partage d'informations. Seuls 9 des 20 pays membres du groupe de travail (Global Task force) de l'Alliance mondiale WeProtect ont des obligations officielles de signalement pour les entreprises technologiques.[53] Le recours à des mesures volontaires de l'industrie laisse d'importantes lacunes en matière de responsabilité, en particulier dans les pays de la majorité mondiale. Les représentants de l'industrie affirment que les systèmes de signalement volontaires peuvent être plus agiles et plus réactifs, mais les parties prenantes s'accordent largement sur la nécessité d'obligations contraignantes.

> « Mais en tant qu'entreprises, elles ne le font souvent que lorsqu'elles y sont obligées. »
>
> *Industrie*[7]

Les évolutions technologiques rapides dépassent les outils juridiques existants, et les tensions entre la protection de la vie privée et la détection proactive demeurent non résolues.[39] Une coordination internationale et une harmonisation législative renforcées, des régulateurs dotés de pouvoirs accrus, des ressources accrues pour les systèmes de protection de l'enfance et les forces de l'ordre, ainsi que des obligations contraignantes pour l'industrie sont nécessaires pour protéger les enfants dans un environnement numérique en rapide évolution.

> « Nous ne pouvons pas résoudre ce problème par des arrestations. »
>
> *Gouvernement*[54]

Ampleur et nature de l'exploitation et des abus sexuels des enfants facilités par la technologie

Depuis la dernière évaluation mondiale des menaces, les préjudices existants se sont maintenus, tandis que de nouveaux risques sont apparus plus rapidement que ne peuvent y répondre les garde-fous juridiques, politiques et technologiques. Le présent chapitre rassemble les données disponibles sur l'ampleur des abus, les caractéristiques des victimes et/ou des survivants, les profils des auteurs et les menaces émergentes, tout en reconnaissant que les données mondiales restent fragmentées, incomplètes et difficiles à comparer. Plusieurs études sur la prévalence de la perpétration, qui seront publiées prochainement, visent à combler les lacunes existantes en matière de données (voir l'annexe). Malgré ces limites, les résultats offrent un éclairage essentiel sur la nature et l'évolution de la menace pour la période 2023-2025 et sert de base aux recommandations formulées plus loin dans le présent rapport.

Panorama des données

> « La vérité, c'est qu'il est vraiment impossible de donner une échelle précise du problème. »
>
> *Industrie*[7]

Les données disponibles sur la CSEA facilitée par la technologie reflètent les progrès collectifs réalisés en matière de coordination, de signalement et de surveillance, et sont essentielles pour comprendre la menace et mobiliser les actions. Cependant, il convient de souligner d'emblée les contraintes persistantes de l'environnement des données, car ces défis conditionnent à la fois l'interprétation des chiffres disponibles et l'analyse qui suit. Les données actuellement disponibles sont fragmentées et partielles. Par exemple, les efforts visant à mesurer la prévalence mondiale sont limités par des lacunes dans la couverture géographique, des définitions non harmonisées, des systèmes de détection et de signalement plus ou moins efficaces et une qualité hétérogène des études. La transparence limitée du secteur rend également difficile l'évaluation des actions menées par les entreprises : par exemple, 60 % des 50 principales plateformes mondiales de partage de contenu ne publient aucune information sur la manière dont elles luttent contre l'exploitation sexuelle des enfants, et parmi celles qui le font, les données sont fragmentées et peu comparables.[55] Les données disponibles peuvent à la fois surestimer le nombre de cas, en raison de doublons ou de classifications erronées, et le sous-estimer, en raison du chiffrement et des plateformes cachées.[7] Les données fiables et représentatives sur les victimes et les auteurs restent limitées, comme nous le verrons plus loin dans ce chapitre. Compte tenu de ces difficultés, nous avons mené des entretiens avec des experts et des défenseurs des victimes afin de combler les lacunes en matière de données et d'obtenir des informations actualisées

et spécifiques au contexte sur les nouvelles tendances et les défis opérationnels. Bien qu'elles ne remplacent pas les données représentatives, la triangulation de ces perspectives avec les ensembles de données et les travaux de recherches existants permet d'obtenir un panorama plus complet et nuancé de la situation.

Ampleur et nature des préjudices

Cette section présente les principaux préjudices qui façonnent le paysage mondial des menaces, notamment les CSAM, le grooming, les abus diffusés en direct, l'IA, l'extrémisme violent en ligne et les développements technologiques tels que le chiffrement de bout en bout, la décentralisation, l'informatique quantique et la réalité étendue (XR).

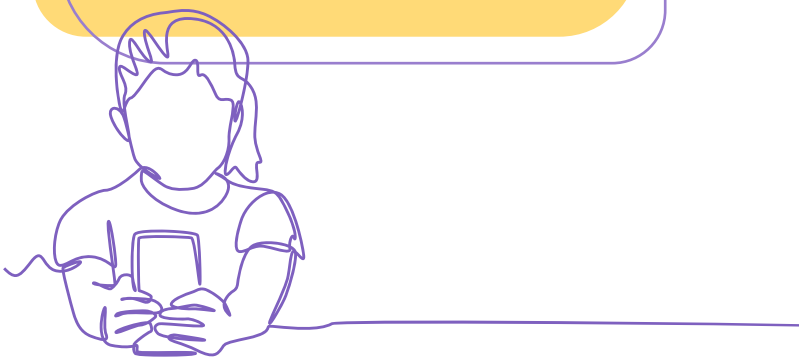
Matériel d'abus sexuels d'enfants

Le CSAM est détecté, signalé et supprimé à des niveaux sans précédent. Comme indiqué précédemment, les tendances en matière de signalement reflètent davantage la capacité de signalement que la prévalence réelle, et la plupart des données sur le CSAM proviennent de plateformes avec beaucoup de fréquentation et donc à revenus élevés, offrant ainsi une vision partielle des préjudices mondiaux. Il est également important de reconnaître que les tendances à la hausse peuvent en partie refléter des évolutions positives, telles que le fait que davantage d>enfants signalent les préjudices subis, que les entreprises améliorent leurs systèmes de détection et que le secteur fait preuve d>une plus grande transparence dans le partage des données. Les données provenant de diverses sources, notamment les rapports obligatoires du National Center for Missing and Exploited Children (NCMEC), les lignes d'assistance téléphonique d'INHOPE et la détection et les signalements proactifs de l'Internet Watch Foundation (IWF), ont des objectifs distincts et utilisent des méthodologies différentes, de sorte que leurs chiffres ne peuvent être combinés de manière significative.

Les chiffres communiqués restent extrêmement élevés.

INHOPE : a reçu plus de 2,5 millions de signalements de CSAM présumé en 2024, soit une augmentation de 218 % par rapport à 2023. Parmi ceux-ci, 65 % ont été confirmés comme étant des contenus illégaux. Cette augmentation est en grande partie due à SafeNet Bulgaria, qui a contribué à hauteur de 1,6 million de signalements.[13]

NCMEC **CyberTipline** : a reçu 20,5 millions de signalements correspondant à 29,2 millions d'incidents en 2024, contre 36,2 millions en 2023. Cette baisse est en partie attribuable aux pratiques de « regroupement » qui regroupent les signalements connexes et à l'impact du chiffrement de bout en bout, qui limite la capacité des entreprises à détecter et à signaler les contenus préjudiciables.[12]



IWF : a revu 424 047 signalements, confirmant 291 273 cas de CSAM ou de liens vers ceux-ci en 2024, soit une augmentation de 6 % par rapport à 2023.[14]

Les types de contenus préjudiciables sont variés et de plus en plus souvent sous forme de vidéos.

NCMEC : près de 63 millions de fichiers ont été signalés en 2024, dont 33 millions de vidéos, 28 millions d'images et 1,8 million dans d'autres formats. Parmi ceux-ci, plus de 51 000 concernaient des enfants en danger imminent nécessitant une intervention urgente.[12]

IWF : a classé 734 048 fichiers uniques comme CSAM, dont plus de 47 000 vidéos et plus de 4 000 images non photographiques interdites.[14]

L'hébergement et la distribution restent concentrés géographiquement pour les contenus qui peuvent être tracés.

INHOPE a signalé que 59 % des serveurs détectés étaient situés aux Pays-Bas et 13 % aux États-Unis, positions qu'ils occupent depuis cinq ans.[13] De même, l'IWF a constaté que plus de la moitié des URL liées à des abus sexuels sur des enfants traitées en 2024 étaient hébergées par des États membres de l'Union européenne, les Pays-Bas, la Bulgarie et la Roumanie hébergeant respectivement 29 %, 9 % et 7 % de ces URL.[14] **L'indice Into the Light** de Childlight met en évidence les niveaux élevés d'hébergement mondial de CSAM provenant des Pays-Bas, ainsi que 4,5 millions de signalements provenant uniquement de l'Inde, du Pakistan et du Bangladesh.[57] La combinaison d'une infrastructure d'hébergement à grande échelle, d'une connectivité à haut débit et de réglementations qui privilégient la liberté d'expression crée des conditions exploitées par les délinquants pour stocker et distribuer des contenus abusifs. L'emplacement de certains contenus ne peut être facilement retracé, car ils sont hébergés sur des réseaux anonymes tels que Tor, conçus pour dissimuler l'origine physique du serveur[11] Le NCMEC a noté que 11 % des signalements **de CyberTipline** avaient une origine inconnue en 2024.[58]

Les modes de distribution ont évolué parallèlement aux efforts de détection. Grâce à la contribution de SafeNet Bulgaria, les forums ont représenté 61 % des signalements reçus par INHOPE en 2024, contre moins de 9 % en 2023, tandis que les signalements provenant de plateformes d'hébergement d'images et de sites web conventionnels ont fortement diminué.[13] Parallèlement, l'IWF a principalement reçu des URL et confirmé 291 270 pages web contenant du CSAM en 2024, soit une augmentation de 5 % par rapport à 2023.[14]

Grooming et incitation en ligne

La sollicitation en ligne, souvent appelée grooming, consiste pour les auteurs à cibler des enfants utilisant Internet afin de les identifier et de les contraindre à des actes sexuels illégaux. En 2024, le NCMEC a recensé 546 000 signalements de sollicitation en ligne, soit une augmentation de 192 % par rapport à 2023, et ce chiffre devrait augmenter à mesure que de plus en plus d'entreprises se conforment à la **loi américaine sur les signalements (U.S. Report Act).**[16]

Intelligence artificielle générative

Les CSAM générés par l'IA, signalés dans les précédentes évaluations mondiales des menaces et dans les entretiens avec des informateurs clés,

continuent de se développer à une vitesse alarmante.[54] Les technologies de deepfake (images ou vidéos générées par l'IA qui représentent de manière réaliste des personnes qui n'ont jamais existé ou qui modifient des photos et des séquences réelles), les chatbots IA (outils de conversation automatisés capables d'usurper l'identité d'enfants ou d'adultes) et les modèles génératifs (systèmes IA capables de produire de nouveaux textes, images ou vidéos à partir de modèles appris) sont utilisés comme des armes pour exploiter les enfants et diffuser du CSAM à grande échelle.[59]

« Si la technologie permet désormais de créer des images et des vidéos qui n'ont jamais existé, comment saurons-nous ce qui est réel à l'avenir, et comment cela changera-t-il la façon dont nous nous faisons confiance en ligne ? »

Garçon de 15 ans, Éthiopie[60]

NCMEC : a enregistré une augmentation de 1 325 % des signalements liés à l'IA entre 2023 et 2024, pour totaliser 67 000 signalements.[12] D'ici juin 2025, les chiffres préliminaires indiquent 440 419 nouveaux signalements impliquant des contenus générés par l'IA et liés à l'exploitation sexuelle des enfants, contre 6 835 au cours de la même période en 2024.[61]

IWF : un seul forum a partagé plus de 3 500 images/vidéos d'enfants modifiées numériquement ou synthétiques en un seul mois.[63]

Thorn : 1 adolescent sur 17 déclare avoir été victime d'images sexuelles deepfake.[62]

Les nouvelles tactiques des délinquants comprennent l'utilisation de l'IA prédictive et de systèmes de recommandation pour identifier et diffuser du matériel d'abus sexuels d'enfants.[63–65] Certains délinquants partagent des modèles d'IA personnalisés, entraînés à partir de matériel d'abus sexuels d'enfants réel, afin de générer du contenu synthétique, tandis que d'autres testent des stratégies de grooming sur des chatbots imitant le langage et les réactions d'enfants.[8,63,66] Dans le même temps, l'IA peut être déployée pour protéger les enfants et faciliter la détection et les enquêtes.

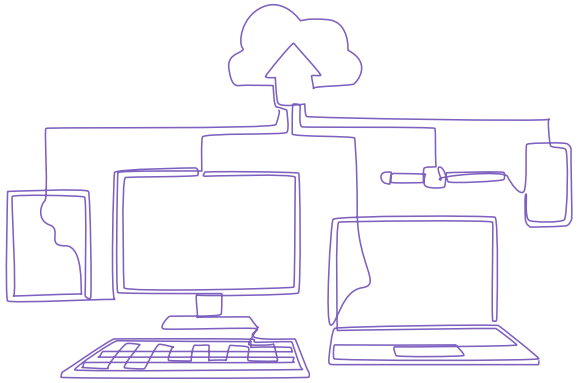


Figure 3. IA : promesses et écueils[6,67,68]

OPPORTUNITÉS

Automatiser la détection des comportements préjudiciables : interrompre les interactions à haut risque, le grooming et le trafic avant que le préjudice ne se produise.

Automatiser la détection du CSAM : identifier, bloquer et supprimer rapidement les contenus préjudiciables.

Soutenir les forces de l'ordre : accélérer les enquêtes, examiner et trier le CSAM, identifier les victimes et les auteurs d'infractions, et réduire l'exposition humaine à des contenus traumatisants.

Sécurité dès la conception : développer et déployer des systèmes et des modèles d'IA générative sûrs.

MENACES

Amplifier les dommages : revictimiser les enfants en créant de nouvelles images à partir de CSAM existants, diffuser des CSAM et générer des guides pour commettre des infractions, contourner les systèmes de vérification de l'âge et amplifier les contenus préjudiciables via des algorithmes.

Générer du CSAM : produire des représentations sexualisées ou explicites d'enfants, en tout ou en partie, y compris des deepfakes d'enfants réels dans des situations sexuelles simulées.

Compliquer la détection et l'application de la loi : entraver l'identification des victimes et des auteurs d'infractions, submerger les systèmes de détection et de suppression et les capacités des forces de l'ordre.

Réduire les barrières techniques et sociales à la maltraitance : permettre la création facile de CSAM, faciliter le grooming en ligne et normaliser l'exploitation et la sexualisation des enfants (par exemple, les applications de « nudification »).

« À mon avis, l'IA pourrait être très utile, mais comme tout outil puissant, elle nécessite des règles de sécurité. Au lieu de la supprimer, nous devrions mettre en place des protections solides et des mesures de sécurité, telles que des filtres, une surveillance et des conseils, afin de garantir sa sécurité pour les enfants et tout le monde. »

Jeune fille de 15 ans, Éthiopie[60]

Extrémisme violent en ligne

Depuis l'évaluation mondiale des menaces de 2023, les groupes en ligne promouvant la violence se sont multipliés, avec une augmentation de 200 % des signalements au NCMEC (plus de 1 300 au total) entre 2023 et 2024.[12] Ces groupes encouragent les enfants à se faire du mal ou à faire du mal à autrui, mettant en évidence de nouveaux liens entre l'exploitation sexuelle, la radicalisation en ligne et les préjudices hors ligne. De nouveaux liens avec les idées suicidaires, les troubles alimentaires, les escroqueries à motivation financière et la traite des êtres humains ont été observés, bien que les recherches restent limitées. Les auteurs s'attaquent souvent aux enfants sur les forums où ceux-ci cherchent de l'aide.[7]

> **« Nous continuerons à voir ces risques se confondre... Je pense que [l'extorsion sexuelle] est un excellent exemple où tant de menaces différentes se sont réunies pour créer ce nouveau préjudice... quand quelqu'un vous contacte et vous dit : 'Salut, tu es mignon, tu veux discuter ?' ...cela se transforme en échange d'images... puis cela peut se transformer en production réelle d'images d'abus sexuels sur des enfants. Ensuite, cela peut se transformer en intimidation et en harcèlement avant de se transformer en chantage réel, avant de pouvoir potentiellement conduire à l'automutilation... »**
>
> *Industrie*[7]

En première ligne de la détection des préjudices : perspectives de PGI sur les groupes « Com »

PGI (Protection Group International) aide les gouvernements, les ONG et les entreprises à détecter et à lutter contre les dangers en ligne, de l'exploitation des enfants à la désinformation en passant par l'extrémisme violent, à l'aide de renseignements humains soutenus par la technologie.

Les groupes « Com » (également appelés le « Com ») sont un archipel de communautés en ligne où les enfants et les jeunes sont ciblés et manipulés pour produire du matériel d'abus sexuels d'enfants, s'automutiler ou même enregistrer des actes violents. Ces groupes sont pour la plupart transnationaux et sont connus sous des noms différents et évolutifs : 764, 676, Harm Nation, Leak Society et CVLT font partie de cette catégorie. Si les auteurs sont souvent eux-mêmes jeunes, principalement des adolescents de sexe masculin, il existe des recoupements avec des sous-cultures extrémistes et marginales, notamment des groupes aux idéologies violentes.

Les tactiques du « Com »

Les auteurs utilisent généralement les plateformes grand public pour identifier les enfants et les adolescents vulnérables, recherchant souvent ceux qui souffrent déjà de troubles mentaux. Par exemple :

- Ils infiltrent les communautés en ligne consacrées à l'automutilation ou aux troubles alimentaires et invitent les enfants à rejoindre des groupes de discussion fermés.
- Ils exploitent les jeux vidéo populaires destinés aux enfants comme des espaces pour rencontrer des victimes potentielles, qu'ils redirigent vers des plateformes de messagerie privée.

Une fois isolés, les jeunes peuvent être confrontés à des menaces, à de la manipulation ou à du chantage. Les victimes peuvent être contraintes d'enregistrer ou de diffuser en direct des actes préjudiciables, notamment des actes d'automutilation, du CSAM, ou la consommation de drogues. Ces contenus sont ensuite compilés dans des « livres de connaissances », qui contiennent également les informations personnelles des victimes. Ces livres circulent parmi les membres de la communauté, et les auteurs acquièrent un statut en fonction du niveau de préjudice qu'ils infligent. Les auteurs créent régulièrement de nouvelles identités en ligne pour éviter d'être détectés.

Impact sur les victimes

- Les victimes subissent souvent de graves dommages psychologiques et vivent dans une peur constante en raison des menaces et du chantage. L'exposition à la coercition et aux demandes violentes peut intensifier les vulnérabilités existantes telles que la dépression, l'anxiété ou les idées suicidaires, conduisant parfois à des actes d'automutilation ou à des tentatives de suicide.
- L'exposition constante à des contenus extrêmes peut normaliser les comportements nuisibles pour les victimes, les amenant parfois à continuer à participer. Certaines victimes passent d'une participation forcée à une implication continue dans des groupes d'agresseurs, allant même dans de rares cas jusqu'à créer leurs propres chaînes et à reproduire les mêmes schémas d'abus.

Abus diffusés en direct

Comme le soulignait déjà l'évaluation mondiale des menaces 2023, l'ampleur et la nature des abus sexuels sur des enfants diffusés en direct – qui se produisent sur les réseaux sociaux grand public ainsi que sur des plateformes de diffusion en direct dédiées – restent importantes et sous-documentées.[69] Des enquêtes menées auprès de délinquants à la recherche de CSAM sur le dark web suggèrent que plus d'un tiers d'entre eux consomment du contenu diffusé en direct, avec une prévalence variable selon les régions.[70] Les enquêtes montrent que les diffusions en direct sont souvent organisées à l'avance, avec de petites transactions financières reliant les consommateurs des régions à revenus élevés aux facilitateurs des juridictions à haut risque.[71] Des projets tels que l'étude « **Scale of Harm** » (Ampleur des préjudices) de l'International

Justice Mission comblent des lacunes importantes en matière de données, mais un suivi plus systématique est nécessaire. Le suivi des échanges financiers est une piste prometteuse pour la détection (voir Prevention).

Technologies en évolution : cryptage, décentralisation, informatique quantique et réalité étendue

Chiffrement de bout en bout

De plus en plus utilisé comme fonctionnalité de confidentialité et de sécurité, le chiffrement de bout en bout garantit que seuls les expéditeurs et les destinataires peuvent voir le contenu des messages. Cependant, lorsqu'il est introduit sans mesures de protection supplémentaires pour les enfants, il rend pratiquement impossible la détection du matériel d'abus sexuels d'enfants ou du grooming et limite considérablement la capacité des forces de l'ordre à identifier les victimes.[72] En décembre 2023, l'une des principales applications de messagerie mondiale, Meta, a activé le chiffrement de bout en bout par défaut, et d'autres plateformes devraient suivre. L'adoption et l'utilisation croissantes du chiffrement de bout en bout ont probablement contribué à une baisse de **7 millions du nombre d'incidents d'exploitation sexuelle d'enfants en ligne** signalés au NCMEC l'année suivante.[12] Plusieurs grandes plateformes ont également réduit le volume des signalements d'environ 20 % en 2024, ce qui soulève des inquiétudes quant à la transparence et la reddition de compte.[73]

Décentralisation

L'informatique décentralisée répartit les tâches entre plusieurs appareils ou systèmes plutôt que de s'appuyer sur une autorité centrale, ce qui permet des connexions et des applications pairs- à-pairs telles que les réseaux sociaux, le stockage de données, les transactions financières et l'apprentissage automatique.[39] Si cette architecture peut améliorer la confidentialité, elle pose également des défis uniques pour prévenir et lutter contre l'exploitation sexuelle des enfants facilitée par la technologie. La décentralisation complique l'identification des suspects, la modération des contenus et la suppression des contenus illégaux.[39] À l'avenir, le principal défi réside dans l'adoption croissante de technologies décentralisées sans garanties adéquates contre les risques déjà observés.[39]

Informatique quantique

L'informatique quantique est un domaine émergent qui permet de traiter les informations à une vitesse exponentiellement plus rapide que les ordinateurs classiques. Bien qu'aucun cas d'utilisation dans le domaine de la CSEA n'ait encore été documenté, les risques futurs pourraient inclure l'accélération de la production de CSAM générés par l'IA ou le piratage des systèmes de cryptage qui protègent actuellement les données des enfants. Il est essentiel de mettre en place des politiques et des considérations de sécurité dès la conception avant que les applications n'arrivent à maturité.[39]

Réalité étendue

Les technologies XR (réalité virtuelle, augmentée et mixte) deviennent plus accessibles et abordables, ce qui augmente les risques d'utilisation abusive et de détournement.[75] Les recherches mettent en évidence les risques d'utilisation abusive, notamment les expériences immersives de CSAM et la normalisation de comportements préjudiciables.[76] Il est essentiel de prendre des mesures préventives avant que la XR ne se généralise. Dans le même temps, la XR est prometteuse en matière de prévention et de formation, car elle offre des simulations réalistes pour les forces de l'ordre et les interventions thérapeutiques. Cependant, les preuves de son efficacité restent limitées.

« … avec la réalité virtuelle, vous allez bientôt pouvoir toucher et sentir, et il y aura des capteurs tactiles placé sur le corps, ce qui constituera un nouveau moyen pour les agresseurs d'infliger des dommages physiques dans l'espace virtuel. »

Survivant[77]

Caractéristiques et vulnérabilités des victimes et/ou des survivants

La section suivante résume ce que l'on sait actuellement sur les victimes et/ou les survivants, tout en soulignant les lacunes persistantes en matière de données. Les informations sur les victimes représentées dans les CSAM restent rares : seule une fraction des millions d'enfants représentés dans les rapports d'INTERPOL sont identifiés, localisés géographiquement ou voient leur âge confirmé.[9] L'ampleur du problème dépasse les capacités des forces de l'ordre, en raison du manque de personnel, des capacités techniques et des ressources financières limitées destinées à identifier les victimes. Les auteurs cachent délibérément les détails permettant de les identifier ou utilisent des technologies de cryptage ou d'anonymisation, ce qui rend l'analyse des images et la recherche de leur source extrêmement difficiles.[7,8] Les contenus signalés représentent de manière disproportionnée des enfants prépubères, tandis que les adolescents sont probablement sous-représentés en raison du manque de recherches sur cette tranche d'âge particulière et de la difficulté à distinguer leurs images de celles de jeunes adultes.[8,9] La stigmatisation, les pratiques de signalement non harmonisées et l'absence de désagrégation des données dans les systèmes administratifs limitent la capacité à comprendre les caractéristiques démographiques et les caractéristiques des victimes. Les groupes marginalisés, notamment les minorités sexuelles et de genre, les enfants handicapés et ceux qui vivent dans des conditions instables ou en institution restent largement absents des données quantitatives, bien qu'ils soient exposés à un risque accru.[8]

> « Nous ne savons pas ce qui arrive aux victimes. »

Agent des forces de l'ordre[79]

Âge et sexe

Conformément aux résultats présentés dans l'évaluation mondiale des menaces de 2023, les filles prépubères restent les victimes les plus fréquemment représentées dans les cas signalés de CSAM. En 2024, les données de l'I See Child Abuse Material -ou ICCAM (littéralement « Je vois du matériel d'abus d'enfant ») ont montré que 98,7 % des cas signalés concernaient des filles, et que 93,2 % d'entre elles étaient des filles prépubères .[13] Les garçons sont surreprésentés parmi les victimes d'extorsion sexuelle, représentant 91 % des signalements reçus par l'IWF en 2023.[14] Des données empiriques suggèrent que les garçons sont davantage victimes d'extorsion sexuelle financière en raison de leurs habitudes de partage d'images ou de l'impression qu'ont les délinquants de leur capacité à payer.[9]

> « Nous avons entendu dire qu'ils ciblent les filles [avec des extorsions sexuelles financières], mais d'une manière différente. Ils ne les ciblent pas pour leur argent. Ils les ciblent pour obtenir des images afin de... les faire chanter. Ce sont les garçons qui sont leur cible. »

Industrie[7]

L'âge reste un facteur essentiel pour comprendre le risque. Les données d'une étude représentative à l'échelle nationale menée auprès de jeunes Australiens âgés de 16 à 24 ans indiquent que les enfants sont généralement confrontés pour la première fois au partage non désiré de leurs propres images à caractère sexuel vers l'âge de 15 ans, bien qu'environ 9 % d'entre eux déclarent avoir vécu leur première expérience avant l'âge de 11 ans.[80] Les données de l'ICCAM montrent une légère augmentation de la proportion de signalements de CSAM impliquant des enfants

prépubères (passant de 90 % en 2023 à 93,2 % en 2024), tandis que les signalements impliquant des adolescents (14-17 ans) et des nourrissons/tout-petits (moins de 3 ans) ont légèrement diminué.[13] INHOPE a également constaté une augmentation du volume de CSAM représentant des enfants de moins de 10 ans.[81]

Vulnérabilités

Conformément aux conclusions de la précédente évaluation mondiale des menaces, les enfants marginalisés, que ce soit en raison de la pauvreté, de leur appartenance à une minorité, de la négligence, de conditions de vie instables ou de leur résidence en milieu rural, sont exposés à un risque disproportionné.[80,82-84] Parmi les autres facteurs de risque figurent les dynamiques familiales qui normalisent les comportements de domination, le manque de connaissances numériques ou de supervision parentale, le manque de soutien social et l'exposition préalable à la violence, aux CSAM et à la pornographie violente.[54,84-86] Les enfants handicapés sont également exposés à des risques accrus d'exploitation sexuelle, des répercussions négatives accrues sur leur santé mentale et des comportements sexuels à risque, ainsi que des obstacles importants à la divulgation, notamment la crainte d'être blâmés par leurs parents, d'être jugés et de perdre leur autonomie.[87-89] Les recherches montrent que les adolescents confrontés à de multiples formes d'abus sont plus susceptibles d'être victimes d'abus sexuels hors ligne et en ligne, ce qui a des répercussions durables sur leur éducation et leur santé mentale.[90-93]

Caractéristiques et comportements des personnes à risque de commettre des infractions et qui ont déjà causé du tort

Les nouvelles données provenant des forces de l'ordre, de la recherche et des communautés de délinquants nous permettent de mieux comprendre qui sont les délinquants, comment ils opèrent et ce qui motive leur comportement. Si la plupart des auteurs sont des hommes adultes, les schémas sont de plus en plus complexes, avec des variations d'âge, de sexe, de géographie, ou dans les motivations et des méthodes. On identifie de plus en plus des enfants et des jeunes qui risquent de commettre des infractions ou qui ont causé du tort et reconnait la nécessité de mener des recherches ciblées, de mettre en place des mesures de prévention et d'apporter un soutien à ce groupe d'âge. Jusqu'à récemment, la recherche se concentrait principalement sur les délinquants adultes identifiés par les systèmes judiciaires ou cherchant de l'aide, ce qui limitait la connaissance des chemins menant à la délinquance et les possibilités d'intervention précoce.

« Nous faisons de notre mieux pour atténuer les risques et réduire les dommages. Mais tant que des personnes continueront à avoir un intérêt sexuel pour les enfants, tant que des personnes voudront exploiter autrui à des fins financières ou autres, nous continuerons à être confrontés à ces problèmes. Ce sont ce que nous appelons des problèmes qui concernent l'ensemble de la société. »

Industrie[7]

Des approches innovantes telles que des études menées directement auprès des délinquants sur le dark web et des estimations de prévalence parmi des échantillons représentatifs d'hommes élargissent la base de données, même si les données fiables et représentatives restent rares.[57,94] Les biais de déclaration et les incohérences dans les définitions limitent également la fiabilité des données.[95] Malgré ces lacunes, la recherche continue de mettre en lumière les vulnérabilités, les technologies, les environnements sociaux et les défaillances systémiques qui favorisent la perpétration d'actes criminels.

Profils des délinquants adultes et modes opératoires

Les données disponibles indiquent que les délinquants qui achètent et échangent du contenu sont principalement des hommes.[96,97] Des enquêtes menées auprès de consommateurs de CSAM sur le dark web montrent que 68 % d'entre eux s'identifient comme des hommes et 17 % ont refusé d'indiquer leur sexe.[94] Dans le cas des abus diffusés en direct, les résultats suggèrent que les consommateurs sont principalement des hommes, principalement basés en Asie, en Europe et en Amérique du Nord, tandis que les producteurs peuvent être aussi bien des hommes que des femmes.[55] Les tendances en matière d'âge varient selon le type d'infraction et la population étudiée. Sur les 4 549 personnes interrogées qui ont déclaré consommer de CSAM sur le dark web, 43 % étaient âgées de 18 à 24 ans.[91] Une autre étude montre que les consommateurs d'abus diffusés en direct ont tendance à être plus âgés.[94,98]

Les auteurs de ces infractions ne sont pas toujours des individus agissant seuls. Il s'agit souvent d'acteurs interconnectés au-delà des frontières : un premier agresseur produit des images ou des vidéos ; d'autres téléchargent ou distribuent le matériel ; et les consommateurs et les acheteurs alimentent la demande qui stimule sa circulation. Les réseaux en ligne échangent, normalisent et amplifient ces abus à l'échelle internationale, ce qui rend extrêmement difficile l'identification des auteurs, malgré des enquêtes spécialisées.[79,99]

Une chaîne mondiale d'abus

Dans le cadre de l'opération Vibora (mars-mai 2025), menée par la police nationale espagnole en collaboration avec INTERPOL et Europol, 20 personnes ont été arrêtées et 68 autres suspects ont été identifiés dans 12 pays en lien avec le CSAM.[100] Dans le cadre de l'opération Cumberland (février 2025), Europol a démantelé une plateforme danoise distribuant du matériel d'abus sexuels d'enfants généré par l'IA, ce qui a conduit à 25 arrestations, à l>identification de 273 suspects et à la saisie de 173 appareils dans 19 pays.[101]

Bien que de nombreuses victimes et auteurs restent non identifiés, les données disponibles sur les cas connus suggèrent qu'une proportion importante des CSAM et autres formes d'abus facilités par la technologie sont produits par des personnes connues de l'enfant.[102] Les rapports de Thorn, s'appuyant sur les données du NCMEC, montrent que deux enfants sur trois sont victimes d'abus de la part d'une personne de leur entourage hors ligne.[10,103] Une meta-analyse réalisée en 2023 portant sur 66 études consacrées à la production de CSAM par les parents souligne que les membres de la famille constituent un groupe important mais sous-estimé à risque de commettre des infractions, produisant généralement du matériel impliquant des enfants prépubères.[104]

> « Il y a un aspect numérique [à l'abus]... il s'agit d'abus sexuels intra-familiaux sur des enfants... les auteurs... même les grands-pères utilisent des services numériques comme WhatsApp... pour discuter en privé et prendre des photos. »

Société civile[11]

Enfants présentant des comportements sexuels préjudiciables

Les comportements sexuels préjudiciables chez les enfants sont reconnus comme un problème croissant, bien que leur prévalence réelle reste incertaine. Avant l'âge de 18 ans, un enfant sur cinq subit des préjudices sexuels, tant en ligne que hors ligne, et plus de la moitié de ces cas se produisent entre pairs.[105,106] Ces comportements peuvent commencer par une exploration entre pairs, mais peuvent parfois dégénérer en infractions plus graves. Un enfant peut par exemple initialement regarder des images à caractère sexuel de pairs du même âge et continuer à rechercher du matériel similaire à l'âge adulte.[9] Les enfants qui affichent des comportements sexuels préjudiciables partagent souvent des vulnérabilités qui se recoupent, telles que des antécédents de victimisation ou d'exposition à des contenus sexuels, des traumatismes, de la négligence, des inégalités sociales et la neurodiversité.[107] Ces vulnérabilités sont souvent aggravées par un manque de sensibilisation, une éducation inadéquate et des systèmes de prévention et de soutien insuffisants.[108] Sans un soutien adéquat, ces comportements peuvent perturber le développement sain, nuire aux relations et causer une détresse psychologique importante. La stigmatisation et l'exclusion peuvent causer des dommages supplémentaires, en particulier lorsque les enfants sont étiquetés comme des délinquants plutôt que reconnus comme des enfants ayant des besoins spécifiques en matière de protection et de développement.[107] Les efforts de prévention et d'intervention existants se sont largement concentrés sur les auteurs adultes. Les interventions axées sur les enfants sont souvent intégrées dans des programmes plus larges de prévention de la violence, ce qui laisse des lacunes dans la compréhension et la réponse.[107] La plupart des interventions commencent trop tard, après que le préjudice a déjà été causé, manquant ainsi une période critique pour la prévention.[108] En négligeant le fait que l'exploration, la mise à l'épreuve des limites et la prise de risques sont des comportements typiques lié à leur développement, les efforts de prévention et d›intervention ne répondent souvent pas aux besoins de ces enfants.[108]

Des données récentes mettent également en évidence les enfants qui ont causé du tort en ligne, notamment en partageant des images à caractère sexuel d'autres enfants sur les plateformes numerques.[80,99,109] Beaucoup n'agissent pas dans l'intention de causer du tort, mais plutôt par ennui, par tentative d'humour ou par attente liée à la masculinité.[7,99,108] Les filles sont plus susceptibles de subir des pressions pour produire du contenu à caractère sexuel, tandis que les garçons sont plus susceptibles de le partager.[99] Les jeunes appartenant à des minorités sexuelles et de genre sont exposés à des risques accrus de chantage et d'intimidation.[110] Il est encore courant de blâmer les victimes. Des enquêtes montrent que près de la moitié des enfants et deux tiers des adultes qui s'occupent d'eux au Cambodge et aux Philippines blâment les victimes lorsque leurs images sont partagées contre leur gré.[111] Comme l'a confié un adolescent : « Il était assez populaire. Cela n'a pas vraiment eu d'effet sur sa popularité...Je pense que cela tient davantage au fait que c'était la fille qui avait envoyé et le garçon n'a pas vraiment subit de répercussions. »

Motivations et voies menant à la perpétration

Les recherches mettent en évidence plusieurs voies menant à la perpétration d'abus sexuels sur des enfants facilités par la technologie. Une forte libido, un intérêt sexuel pour les enfants, la neurodiversité et une dysrégulation émotionnelle sont documentés comme facteurs de risque.[94,108] Dans les données des lignes d'assistance téléphonique, certains délinquants ont déclaré que leur propre victimisation pendant l'enfance avait contribué à leur comportement abusif ultérieur, le traumatisme agissant à la fois comme motivation et rationalisation.[52,112]

De nouvelles données issues d'enquêtes permettent de mieux comprendre ces motivations. Une étude réalisée en 2024 auprès de 4 549 délinquants du dark web a révélé que :

- 30 % étaient motivés par un intérêt sexuel pour les enfants,
- 15 % cherchaient à réguler des émotions telles que la solitude ou la dépression,
- 10,6 % avaient le désir de comprendre leur propre expérience de la maltraitance, et
- 6,3 % recherchaient du matériel représentant leur propre abus.

Il est à noter que près de 40 % des délinquants ont déclaré avoir consommé de manière intensive de la pornographie adulte avant de passer à la CSAM.[94] Cela concorde avec d'autres études qui montrent que les délinquants commencent souvent par consommer de la pornographie adulte, puis recherchent de la nouveauté et de la « variété ».[95,113] La consommation de pornographie de plus en plus violente ou extrême peut découler d'autres facteurs problématiques à l'origine de comportements sexuels nuisibles et interagir avec ceux-ci, reflétant un schéma de désensibilisation. Des recherches supplémentaires sont nécessaires pour comprendre ces interactions complexes et les voies menant à l'escalade et à la perpétration.

Les motivations financières sont importantes : il existe des preuves que les CSAM sont utilisés pour générer du trafic sur Internet, tandis que des crimes tels que l'extorsion sexuelle, la diffusion en direct et la traite des êtres humains, souvent facilités par l'IA générative, sont très lucratifs.[2,115] Les auteurs d'extorsion sexuelle financière sur des enfants sont souvent basés dans des pays à faible et moyen revenu tels que le Nigeria, les Philippines et la Côte d'Ivoire, tandis que les victimes se trouvent généralement dans des pays à revenu élevé.[116] En 2024, le NCMEC a signalé environ 100 cas d'extorsion sexuelle financière d'enfants par jour, les garçons étant disproportionnellement visés.[117] L'IWF a également signalé que 91 % des victimes d'extorsion sexuelle étaient des hommes.[117]

> « Les gens pensent souvent que les délinquants sont uniquement motivés par la satisfaction sexuelle, mais de plus en plus, leur motivation est financière. »
>
> *Industrie*[7]

Méthodes et technologies utilisées pour commettre les infractions

Les méthodes utilisées pour commettre ces infractions sont dynamiques et influencées par l'évolution des technologies. Les auteurs exploitent l'anonymat, le cryptage et les failles des plateformes pour partager du CSAM sur le web ouvert et le dark web.[118] Ils dissimulent le contenu à l'aide de manipulations de liens, de réseaux de diffusion de contenu, de sites web doppelgänger (masqués) et d'échanges chiffrés sur les réseaux sociaux afin d'éviter d'être détectés et supprimés.[11,119]

« Auparavant, cela ne se trouvait que dans des forums obscurs ou sur le dark web... mais ces deux dernières années, on a assisté à une augmentation considérable de la disponibilité [du CSAM]. »

Industrie[7]

Les algorithmes peuvent également faire apparaître du contenu préjudiciable ou mettre en relation des enfants avec des auteurs d'infractions. Dans le même temps, les outils d'IA, la technologie deepfake et les applications « nudify » (logiciels qui créent de fausses images nues ou sexuellement explicites à partir de photos de personnes réelles) permettent la production d'images synthétiques à caractère sexuel, qui peuvent être utilisées pour contraindre les victimes à produire de véritables CSAM.[13,118,121] Ce schéma implique généralement un premier contact et un conditionnement sur les réseaux sociaux, les jeux vidéo et les plateformes de messagerie grand public, suivis d'un passage à des environnements cryptés ou anonymes pour intensifier l'abus.[120]

« Il n'existe aucune plateforme sûre, les délinquants utilisent toutes les plateformes... lorsque nous leur demandons où ils contactent les enfants, ils répondent évidemment sur le web ouvert, les réseaux sociaux et les plateformes de jeux, là où se trouvent les enfants. Les enfants [les jeunes enfants] ne sont pas sur le dark web. »

Société civile[11]

Prévention

Nous utilisons une définition large de la prévention, qui englobe toutes les actions visant à:

1 Empêcher les enfants d'être victimes d'exploitation et d'abus ou de causer du tort à d'autres enfants,

2 Prévenir la re-victimisation et la récidive, et

3 Réduire les conséquences néfastes pour les enfants qui ont déjà subi des abus et assurer la réadaptation de ceux qui ont causé du tort.

Cette définition inclut les actions qui peuvent être menées après que le préjudice ait été causé, souvent décrites comme de la prévention ou réponse tertiaire. Si ces efforts bénéficient souvent d'une attention et de ressources accrues, il convient d'accorder une plus grande attention à la lutte contre les causes profondes, à renforcer les facteurs de protection et à prévenir es préjudices avant qu'ils ne se produisent. Les efforts de prévention doivent s'étendre à tous les niveaux de l'environnement de l'enfant, y compris ses pairs, sa famille, sa communauté, les institutions et la société en général, et s'adapter à un paysage technologique en constante évolution.[30] Des réponses créatives et intersectorielles démontrent que la prévention est possible, plusieurs d'entre elles étant menées ou inspirées par les enfants et les survivants eux-mêmes. Les technologies émergentes ont introduit de nouveaux risques, mais elles offrent également des possibilités de protection.

Une prévention efficace doit commencer par s'attaquer aux facteurs sociaux, structurels et financiers à l'origine des préjudices. Elle doit tenir compte de la manière dont des facteurs tels que l'âge, l'orientation sexuelle et l'identité de genre, le handicap, la neurodiversité, l'origine ethnique, le statut d'autochtone ou de migrant, les conditions socio-économiques et le niveau d'éducation se combinent pour déterminer les risques de préjudice ou de comportement préjudiciable pour les enfants. Les déséquilibres de pouvoir, la pauvreté, le faible niveau de culture numérique et une supervision parentale limitée peuvent accroître les risques pour les enfants.[123,124] Les normes sociales néfastes, la stigmatisation, la honte et le blâme des victimes peuvent dissuader celles-ci de se manifester et de demander de l'aide, tandis que la faiblesse des lois et de la gouvernance favorise la prolifération des abus.[85,91,121] Les facteurs économiques, notamment l'extorsion sexuelle financière et les revenus provenant du trafic et de la publicité en ligne, doivent également être pris en compte. La prévention de l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie nécessite enfin un engagement politique et des investissements soutenus dans les systèmes, les ressources et les processus qui protègent les enfants. Les principaux facteurs favorisant la prévention sont les suivants :

- Un engagement politique soutenu et un financement dédié qui donne la priorité à la sécurité et au bien-être des enfants,
- Une gouvernance numérique solide et des prises de responsabilités à tous les niveaux du gouvernement,

- De la recherche et les données pour informer la prévention et hiérarchiser les ressources,
- Des systèmes solides de protection de l'enfance, dotés de professionnels formés capables de détecter les risques à un stade précoce et d'apporter une aide adaptée aux enfants et tenant compte des traumatismes subis,[121]
- Des normes sociales favorables à la prévention, qui reconnaissent que la CSEA facilitée par la technologie peuvent être évitée, encouragent le signalement et incitent les personnes ayant des pensées ou des comportements sexuels préjudiciables à demander de l'aide. [125]
- Une collaboration mondiale et intersectorielle pour coordonner la prévention, renforcer la responsabilité et harmoniser la terminologie, les normes en matière de données et les systèmes de surveillance.

> « Si vous donnez un appareil et un accès à un téléphone portable ou à Internet à votre enfant… vous lui ouvrez la porte d'un environnement social rempli d'adultes. Est-ce que vous feriez cela chez vous ? Vous venez d'ouvrir la porte et de dire 'Bienvenue à tous !' »
>
> *Société civile*[11]

Combler le déficit de financement

> « Je constate des occasions manquées car le financement est très limité en ce moment, surtout [avec] ce qui se passe dans le monde… Tout le monde se bat [pour] obtenir des fonds, ce qui ne facilite pas la collaboration… Nous devrions travailler davantage ensemble pour prévenir ces crimes. »
>
> *Société civile*[11]

Malgré l'ampleur et la complexité croissantes de la CSEA facilitée par la technologie, il existe un « déficit important de financement mondial– et qui s'aggrave » destiné à la prévention, la réponse et la recherche. Safe Online identifie le sous-financement chronique comme « le plus grand obstacle à la réalisation d'un avenir numérique sûr, inclusif et éthique pour les enfants ».[126] Le décalage entre les investissements dans la prévention et le coût des dommages est flagrant. La violence à l'égard des enfants peut coûter aux pays jusqu'à 11 % de leur PIB, dépassant dans certains cas six fois les dépenses nationales de santé.[126] Aux États-Unis, plus de 5 milliards de dollars sont dépensés chaque année pour incarcérer des adultes condamnés pour des crimes sexuels contre des enfants, soit plus de 3 000 fois le budget consacré à la recherche sur la prévention de la maltraitance des enfants.[127] Les pays à faible et moyen revenu sont particulièrement sous-financés, dépendant souvent d'un financement à court terme basé sur des projets plutôt que de réponses nationales durables.[128] Pour combler le déficit de financement, il faut des approches innovantes, notamment un financement catalytique provenant de sources philanthropiques, un cofinancement des gouvernements, des investissements soutenus par des institutions financières internationales et d'autres agences multilatérales, ainsi que des mécanismes plus

solides pour le financement à long terme. Des fonds sont également nécessaires pour renforcer les systèmes nationaux essentiels à la prévention, notamment la santé, l'éducation, la protection de l'enfance, les services sociaux et les systèmes juridiques. Compte tenu de la réalité d'un environnement financier contraint, il est essentiel d'utiliser plus efficacement les ressources disponibles, en coordonnant mieux les efforts de prévention entre les secteurs, en utilisant des données et des résultats scientifiques pour hiérarchiser les investissements, et en adaptant et testant des interventions basée sur des données, notamment celles issues du programme de lutte contre la violence à l'égard des enfants (Violence Against Children Agenda).[9] Des analyses coûts-avantages sont également nécessaires pour démontrer que la prévention est plus rentable que les réponses réactives à la CSEA facilitée par la technologie.

> « Il y a beaucoup d'éléments intéressants pour... harmoniser davantage le dialogue Nord-Sud, pour faire entrer le monde universitaire dans la sphère des praticiens... [mais] je pense malheureusement que le paysage financier n'est pas propice à l'amélioration de cette situation. »
>
> *Société civile*[11]

Renforcer la base de données factuelles pour la prévention

> « C'est une phrase un peu automatique de dire... que nous avons besoin de plus de données, mais à un moment donné, nous devons prendre conscience du fait que... Si vous avez plus de 500 [études sur l'exploitation sexuelle des garçons], il est injuste de dire qu'il n'y a tout simplement pas de données. C'est juste que la qualité des données est souvent médiocre. »
>
> *Académiques*[8]

Des données scientifiques sont essentielles pour comprendre les risques émergents, évaluer les stratégies de prévention et orienter les investissements. Une approche de santé publique peut guider ce processus : (1) définir et surveiller le problème et sa prévalence ; (2) identifier les facteurs de risque et de protection ; (3) concevoir, tester et évaluer des stratégies de prévention ; et (4) partager les enseignements tirés et généraliser les mesures efficaces.[123] Pour traduire la recherche en une prévention plus efficace, il faut une recherche coordonnée et un partage des données entre les secteurs et les pays. **L'initiative Data for Change**, lancée en 2022 et qui regroupe aujourd'hui 120 organisations, vise à recenser les bonnes pratiques, à réduire les obstacles au partage d'informations et à donner la priorité aux données provenant des pays de la majorité mondiale.[130] L'initiative met l'accent sur l'adaptation des approches à des contextes spécifiques et l'implication de jeunes chercheurs dans les pays à revenu faible et intermédiaire, afin de rendre les données mondiales plus inclusives et exploitables. La note d'information de l'UNICEF **sur la mesure de la violence à l'encontre des enfants facilitée par la technologie, conformément à la classification internationale de la violence à l'encontre des enfants**, fait progresser les efforts visant à améliorer la qualité et la comparabilité des données mondiales.[131]

Pour rester informé des nouvelles tendances et des dernières données mondiales sur les stratégies de prévention efficaces, consultez les ressources actualisées en annexe.

Transformer les données en actions pour mettre fin à la violence sexuelle envers les enfants : le cadre mondial de revue systématique et de connaissances pratiques du Safe Futures Hub

Lancé en septembre 2023, le Safe Futures Hub est codirigé par la Sexual Violence Research Initiative (SVRI), Together for Girls et WeProtect Global Alliance.[132–135] Sa mission est de mettre fin à la violence sexuelle envers les enfants en promouvant des solutions fondées sur des données, des résultats scientifiques, les connaissances des praticiens et des approches communautaires.

Début 2026, le Safe Futures Hub, en collaboration avec l'université d'Oxford, lancera la **Living Systematic Review**, une ressource mondiale mise à jour qui synthétise les résultats scientifiques sur les mesures efficaces pour prévenir la violence sexuelle envers les enfants. La **Living Systematic Review** applique des méthodes rigoureuses et transparentes pour identifier, évaluer et résumer les nouvelles études d'intervention, garantissant ainsi aux décideurs politiques, aux praticiens et aux chercheurs l'accès aux résultats les plus récents. Contrairement aux revues statiques, elle évoluera en temps réel, comblant ainsi le fossé entre la recherche et la pratique. S'appuyant sur le rapport factuel **Building Safe Futures** 2024 et son appel à une action plus forte et fondée sur des preuves, cette ressource guidera les investissements dans des stratégies efficaces et adaptées au contexte. En mettant en avant les interventions qui fonctionnent, **la revue systématique évolutive** du Safe Futures Hub permettra aux parties prenantes de développer et d'adapter des solutions qui protègent les enfants contre la violence sexuelle.

En décembre 2025, le Safe Futures Hub lancera deux nouvelles ressources afin de renforcer la reconnaissance et l'utilisation des connaissances fondées sur la pratique (Practice-based knowledge ou -PbK) dans la prévention et la lutte contre la violence sexuelle envers les enfants.

- **Le document de référence** explique ce qu'est le PbK et pourquoi il est important pour prévenir et lutter contre la violence sexuelle envers les enfants, en montrant comment il permet de faire entendre les voix sous-représentées, de renforcer les pratiques et de valoriser à la fois l'expertise des praticiens et l'expérience vécue.
- **Le cadre d'orientation** propose des outils et des processus concrets pour aider les praticiens à recueillir, utiliser et partager les connaissances pratiques de manière sûre, éthique et pratique.

Dans le contexte de la prévention et de la lutte contre la violence sexuelle envers les enfants, les connaissances pratiques désignent les enseignements tirés de l'expertise acquise sur le terrain et de la participation directe à des programmes, des services ou des actions de sensibilisation. Alors que la recherche montre ce qui fonctionne, les connaissances pratiques expliquent comment cela fonctionne, pourquoi cela fonctionne et comment continuer à faire fonctionner ces méthodes dans des contextes complexes et changeants. Ensemble, les connaissances pratiques et la recherche peuvent rendre les stratégies plus efficaces, plus pertinentes et mieux adaptées aux contextes réels.

Concevoir le cadre de prévention

Au fil des consultations, un message commun s'est dégagé : nous devons agir maintenant. Il est nécessaire de comprendre l'ampleur et la nature de la CSEA facilitée par la technologie, mais cela ne suffit pas. Le défi central auquel beaucoup dans ce domaine continuent de faire face – « par où commencer ? » – a été le moteur de ce cadre de prévention.

Le cadre de prévention a été élaboré pour compléter le modèle de réponse nationale de l'Alliance mondiale WeProtect, qui fournit une structure d'action aux niveaux national et systémique. Ensemble, ils cherchent à guider l'action mondiale pour lutter contre la CSEA facilitée par la technologie.[29] Le cadre s'appuie également sur d'autres modèles bien établis :

- Le modèle socio-écologique, qui souligne que les risques et les protections existent à plusieurs niveaux de l'environnement de l'enfant ;[30] et
- L'approche de prévention en matière de santé publique, qui définit la prévention à différents niveaux, depuis les approches visant l'ensemble de la population jusqu'aux mesures ciblées pour les personnes exposées au risque de subir ou de causer un préjudice.[123]

Le cadre s'appuie également sur les normes internationales et régionales relatives aux droits de l'enfant, notamment la Convention des Nations unies relative aux droits de l'enfant et les observations générales 16, 24 et 25, ainsi que le Pacte mondial pour le numérique.[24,33,136] Il a été élaboré conjointement dans le cadre d'un processus participatif impliquant des jeunes, des survivants et un comité directeur d'experts représentant les gouvernements, la société civile, l'industrie et les agences intergouvernementales. Les parties prenantes ont apporté leur contribution par le biais d'ateliers et de commentaires écrits.

> « **Lorsque nous menons des efforts de prévention, je pense que nous devons impliquer toutes les parties prenantes... les survivants, les personnes ayant une grande expérience, les industries technologiques, les institutions religieuses, les leaders communautaires, les enseignants, les parents, les mentors de jeunes, les ONG, la société civile et même les organisations régionales comme l'Union africaine, l'ONU et INTERPOL.** »
>
> *Société civile[11]*

Le cadre de prévention s'articule autour de quatre domaines d'action interdépendants :

- Participation et leadership des enfants
- Éducation et soutien communautaires
- Sécurité numérique
- Droit, politique et justice

L'ordre dans lequel ils sont présentés reflète une approche socio-écologique, qui commence par les enfants et progresse vers la communauté, les institutions, les gouvernements et les acteurs mondiaux. Les domaines d'action sont répartis sur trois niveaux de prévention : primaire (protection proactive), secondaire (détection et prévention des dommages) et tertiaire (intervention et soutien après les abus). Les facteurs favorables tels que la recherche et le financement sont essentiels et doivent être pris en compte en permanence afin de garantir l'efficacité et la durabilité de toutes les actions.

Au lieu de classer les interventions en fonction de la force des résultats scientifiques disponibles, ce qui n'est pas encore possible, ce cadre présente des recommandations thématiques afin d'aider les parties prenantes à identifier les mesures de prévention pertinentes pour leur contexte et leur expertise. Le cadre met en évidence les approches fondées sur des preuves lorsqu'elles sont disponibles et renvoie dans le cas contraire aux recommandations d'experts, aux bonnes pratiques et aux pratiques innovantes qui doivent être évaluées plus en détail.

> « **Une approche de santé publique est désormais nécessaire, avec la mise en place d'un système visant à prévenir les actes de violence, à détecter et à traiter les crimes, mais aussi à soutenir les victimes et leurs familles.** »
>
> *Académiques[8]*

Avis d'experts sur les priorités en matière de prévention tirés de l'évaluation mondiale des menaces 2025

Notre enquête en ligne menée auprès de 77 professionnels travaillant à la lutte contre l'exploitation sexuelle des enfants à des fins sexuelles facilitée par la technologie (61 % dans le secteur à but non lucratif, 19 % dans le secteur public, 16 % dans le secteur privé et 3 % dans des organismes statutaires indépendants) a confirmé un soutien massif en faveur des quatre domaines d'action. Les personnes interrogées ont appelé à une meilleure compréhension du comportement, des motivations et du profil des auteurs (47 %) ; les causes profondes et les facteurs systémiques des préjudices (45 %) ; et le point de vue des enfants sur l'utilisation des technologies (39 %). Les principales priorités identifiées pour intensifier les efforts de prévention étaient un financement flexible à long terme (87 %), la formation et le soutien technique du personnel (58 %) et l'accès à des outils et des conseils open source axés sur les enfants (50 %).

Bien qu'elles soient basées sur un petit échantillon d'experts, ces conclusions reflètent un large consensus sur les priorités en matière de prévention et sur le besoin urgent d'investissements, de renforcement des capacités et de collaboration.

Mettre la prévention en pratique : le modèle « du fromage suisse »

Le modèle « du fromage suisse » offre un prisme puissant pour comprendre comment ce cadre de prévention peut être appliqué dans la pratique.[137] Largement utilisé dans des domaines où la sécurité est cruciale, tels que l'aviation, la médecine et l'ingénierie, ce modèle souligne que les dommages graves résultent rarement d'un seul point de défaillance. Au contraire, les dommages surviennent lorsque plusieurs faiblesses des systèmes de protection se conjuguent. Chaque « tranche » de fromage suisse représente une couche de protection, par exemple les mesures de sécurité numérique, les lois, les politiques et les mécanismes judiciaires. Chaque tranche comporte des « trous » qui représentent des points faibles. Un seul trou ne cause pas nécessairement de préjudice, car les autres couches font office de barrière, mais lorsque les trous de plusieurs couches s'alignent, des préjudices graves peuvent survenir.

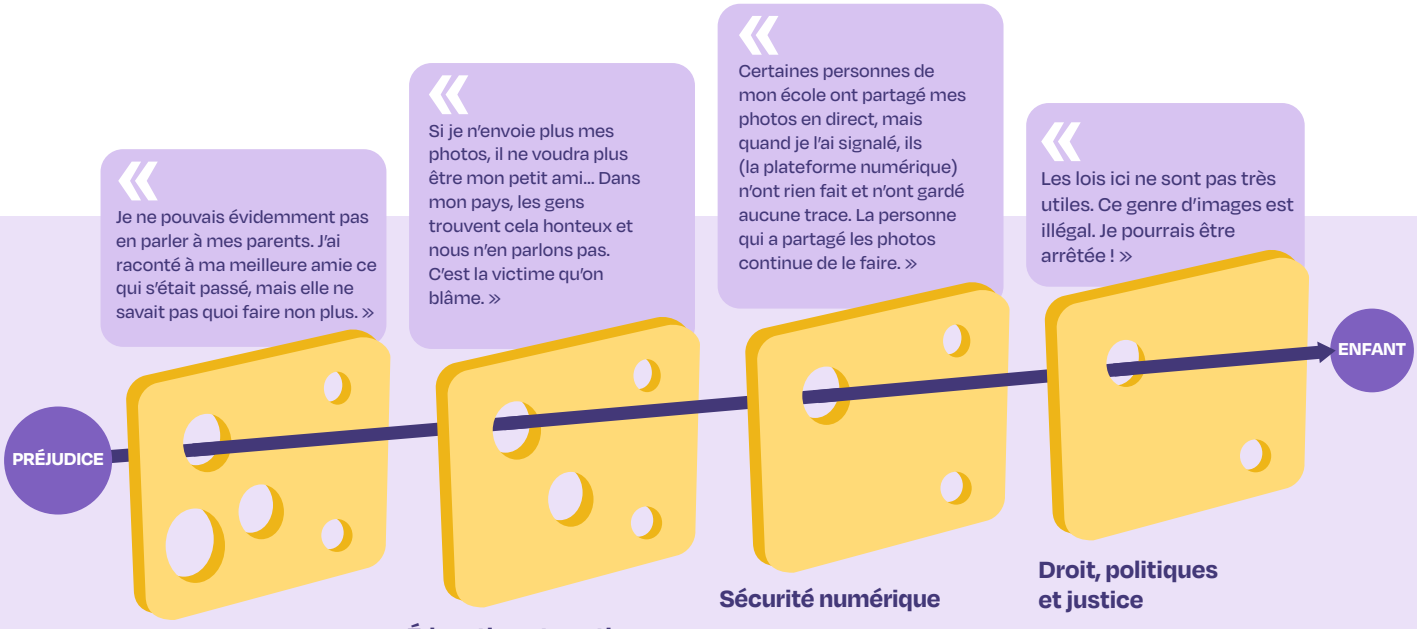
Appliqué à l'exploitation sexuelle d'enfants facilitée par la technologie, le modèle du fromage suisse met en évidence trois points importants :

- Chaque fois qu'un enfant est victime d'abus sexuels commis par des étrangers à l'aide de la technologie, cela reflète une défaillance du système et de multiples occasions manquées d'intervenir.
- Aucun acteur ou secteur ne détient à lui seul toutes les solutions. Plusieurs niveaux de prévention doivent fonctionner ensemble.
- La prévention nécessite un apprentissage et une adaptation continus afin d'identifier les faiblesses de la protection, la gravité et l'urgence des conséquences potentielles, ainsi que les ressources disponibles pour combler les lacunes ou renforcer d'autres couches de protection.

Utilisés conjointement, le cadre de prévention et le modèle du fromage suisse fournissent une structure et une méthode. Alors que le cadre de prévention englobe toutes les formes de CSEA facilitées par la technologie, le modèle du fromage suisse peut aider les parties prenantes à hiérarchiser les actions, à évaluer les risques et à identifier les faiblesses qui contribuent à un incident ou à un type de préjudice particulier. Ensemble, ils déplacent l'attention des solutions isolées vers la mise en place de systèmes résilients avec des protections à plusieurs niveaux pour assurer la sécurité des enfants.

Scénario : Amal est au lycée. Elle a récemment rompu avec son partenaire, qui a le même âge qu'elle. Pour se venger, son partenaire a publié des photos intimes d'Amal en ligne, puis d'autres personnes les ont diffusées dans son école. Ce qui est arrivé à Amal est le résultat d'échecs à plusieurs niveaux. Voici comment les choses se sont déroulées de son point de vue.

Figure 4 . Visualisation du modèle du fromage suisse : comprendre les risques liés aux contenus sexuels autoproduits impliquant des enfants



Participation et leadership des enfants

- Des pairs "soutiens" formés pour recevoir les plaintes et orienter les enfants vers les services d'appuis.
- Conception, menée par des enfants et des survivants, de supports d'éducation et de sensibilisation, de canaux de signalement et de fonctionnalités de sécurité numérique.

Éducation et soutien communautaires

- Programmes scolaires sur les relations saines, la sexualité et la sécurité numérique.
- Soutien précoce aux enfants exposés au risque de subir ou de causer des préjudices.
- Formation des éducateurs et politiques scolaires claires pour la prévention et la réponse.
- Campagnes de sensibilisation communautaires pour faire évoluer les normes, réduire le blâme des victimes et encourager le signalement.

Sécurité numérique

- Évaluations d'impact sur les droits de l'enfant et fonctionnalités de sécurité intégrés dès la conception lors du développement des plateformes (par exemple, détection de nudité, fenêtres contextuelles d'avertissement qui interrompent le partage à risque et encouragent la recherche d'aide).
- Options de signalement accessibles qui fournissent un retour rapide, renvoient vers des services de soutien et permettent de retirer rapidement les contenus ou comptes préjudiciables.

Droit, politiques et justice

- Lois respectueuses des droits qui protègent les victimes et évitent de criminaliser les comportements consensuels entre pairs d'âge proche.
- Autorités de régulation habilitées à contrôler le respect des obligations par l'industrie, enquêter sur les abus et imposer des sanctions.
- Une justice adaptée aux enfants et un accès à des recours effectifs grâce à des policiers, des juges et des procureurs formés.

Domaines d'action en matière de prévention

Participation et leadership des enfants

> « La voix des enfants doit être entendue à chaque étape de la prévention, de la détection et de la réponse. »

Survivante, Philippines[138]

Les enfants et les survivants doivent avoir la possibilité de partager leurs points de vue et d'influencer les politiques, les programmes et les services qui les concernent grâce à une participation sûre et significative.

Les partenariats avec des organisations dirigées par des enfants et axées sur les enfants peuvent promouvoir une participation sûre, détecter les risques et les préjudices à un stade précoce et éclairer des interventions efficaces et centrées sur les enfants.

Des efforts doivent être faits pour impliquer tous les enfants, en particulier ceux issus de milieux marginalisés, en reconnaissant que les enfants courent le risque d'être victimes de préjudices et de causer des préjudices à d'autres enfants.

Principes pour une participation sûre et significative

> « Ils [les enfants] sont les personnes les plus vulnérables et les plus indispensables pour résoudre le problème. »

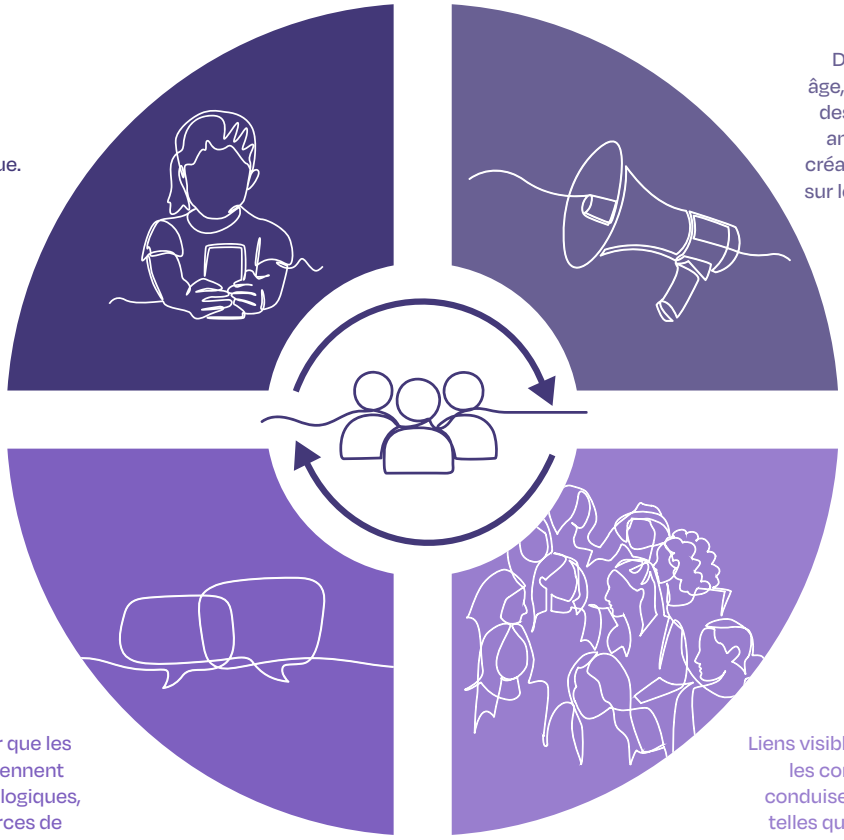
Survivant, Philippines[138]

L'article 12 de la Convention des Nations Unies relative aux droits de l'enfant affirme le droit de chaque enfant d'être informé, d'exprimer son opinion et de participer aux décisions qui affectent tous les aspects de sa vie.[33] **Le modèle Lundy** (voir figure 5) fournit un cadre pratique pour l'application de l'article 12 afin de soutenir la participation significative des enfants.[139] Les enfants et les jeunes peuvent aider à identifier les risques émergents et à élaborer des stratégies de prévention proactives. Dans le cadre d'une campagne mise en œuvre en Indonésie, au Népal et aux Philippines, l'organisation de défense des droits des

enfants Kindernothilfe a élaboré un **guide et une boîte à outils** pour soutenir la participation significative des enfants et des jeunes à la promotion de la prévention et de la protection contre la violence en ligne.[140,141]

L'UNICEF a élaboré un **guide Spotlight** qui partage les meilleures pratiques pour impliquer les enfants dans les évaluations d'impact des droits numériques des enfants.[142]

Figure 5. Caractéristiques d'une participation significative appliquées en ligne[143]



ESPACE
Des forums sûrs, accessibles et adaptés aux enfants, où ceux-ci peuvent discuter des risques liés au numérique.

VOIX
Des outils adaptés à leur âge, tels que des sondages, des avatars, des enquêtes anonymes et des médias créatifs, pour en savoir plus sur les expériences en ligne des enfants.

PUBLIC
Des voies directes pour que les idées des enfants parviennent aux entreprises technologiques, aux régulateurs, aux forces de l'ordre et aux décideurs politiques.

INFLUENCE
Liens visibles montrant comment les contributions des enfants conduisent à des améliorations, telles que de meilleurs outils de signalement, des fonctionnalités de confidentialité renforcées ou des programmes de prévention en milieu scolaire.

La sécurité, la qualité et l'intérêt supérieur des enfants doivent toujours être prioritaires lorsque l'on travaille avec eux. La participation des enfants ne doit avoir lieu que lorsque le personnel, les mesures de protection et les services d'aide tenant compte des traumatismes sont en place pour les protéger contre tout préjudice. Si cela n'est pas possible, il convient de s'appuyer sur les connaissances des jeunes, des adultes et des organisations qui peuvent représenter les points de vue des enfants, ainsi que sur les données existantes, les recherches et les bonnes pratiques.

Impliquer les enfants et les survivants dans la prévention

> « Je pense que les ONG créées par des jeunes et pour les jeunes seront vraiment utiles. Ces organisations pourraient sensibiliser les jeunes de manière plus naturelle, car les conseils viendraient d'autres jeunes. »
>
> *Homme de 17 ans, Pakistan*[60]

Parmi les initiatives visant à impliquer les enfants et les jeunes dans la prévention, on peut citer :

- **Mtoto News**, une plateforme numérique et médiatique basée au Kenya qui facilite la défense des droits des enfants et permet à plus de 100 000 enfants de dialoguer directement avec leurs dirigeants sur des questions telles que les abus sexuels envers les enfants en ligne et hors ligne.[144]
- **L'indice de bien-être numérique** de la Snap Foundation, qui invite les jeunes de six pays à partager leurs réflexions sur leur bien-être psychologique et leurs expériences sur les plateformes en ligne, permettant ainsi d'identifier des informations importantes pour la prévention.[45]
- **BeSmartOnline,** le centre officiel pour un Internet plus sûr du gouvernement maltais, guidé par un panel de jeunes qui aide à identifier les nouveaux risques en ligne et à concevoir conjointement des stratégies efficaces de sensibilisation.[145,146]

Le leadership des jeunes en matière de sécurité en ligne : perspectives de VoiceBox

VoiceBox est une entreprise sociale et une plateforme de contenu basée au Royaume-Uni et dirigée par des jeunes, qui aide les jeunes créateurs âgés de 13 à 25 ans à s'épanouir et à façonner des environnements numériques plus sûrs, centrés sur leurs expériences vécues.[147] Grâce à un réseau mondial couvrant plus de 50 pays, VoiceBox amplifie la diversité des points de vue et peut souvent identifier les risques émergents en ligne plus rapidement que les recherches traditionnelles, servant ainsi de « système d'alerte précoce » pour les décideurs politiques et les leaders du secteur. Cela permet aux décideurs de disposer en temps réel d'informations fiables fournies par les jeunes sur l'évolution des menaces.

VoiceBox recueille des informations honnêtes et non filtrées auprès des jeunes sur les défis complexes liés à la sécurité en ligne, notamment la maîtrise des médias, les dangers en ligne et les risques numériques émergents. Son approche combine des opportunités de leadership pour les jeunes avec un soutien solide en matière de protection et de prise en charge des traumatismes. VoiceBox utilise des groupes de discussion animés par des pairs, des entretiens et des méthodes créatives de collecte d'informations (telles que l'art, les vidéos et la poésie) pour permettre aux jeunes de partager leurs expériences de manière sûre et authentique. Cette approche a mis en lumière des questions telles que les compagnons IA et les plateformes par abonnement.[44]

Les enfants victimes de discrimination intersectionnelle, tels que les minorités sexuelles et de genre et les enfants handicapés, sont exposés à des risques et à des préjudices uniques en ligne, mais ils sont souvent exclus des politiques et des programmes.[11]

> « Si ces questions ne sont pas suffisamment prises en compte dans la conception des interactions et des politiques, nous risquons de passer à côté de cette population sous-représentée. »
>
> *Société civile*[11]

Il est important de consulter les enfants marginalisés et ceux qui ont des besoins spécifiques et qui peuvent utiliser les technologies numériques différemment de leurs pairs.[8] Par exemple, les enfants sourds, qui dépendent souvent de la communication vidéo, sont exposés à des risques uniques en ligne et peuvent avoir moins de possibilités de reconnaître ou de signaler une exploitation potentielle.[11] Il est essentiel de mettre en place des stratégies de communication accessibles, adaptées et inclusives pour garantir leur sécurité en ligne. Voici quelques exemples d'initiatives menées par des survivants ou inspirées par eux :

- **Disrupting Harm** génère des données de haute qualité sur les préjudices numériques subis par les enfants et les jeunes dans 25 pays répartis dans 6 régions. Le projet utilise des processus participatifs tenant compte des traumatismes et suivant des directives éthiques strictes et des procédures de protection des enfants. La première phase a révélé que près d'un enfant sur trois ne signalait pas les préjudices subis, près de la moitié d'entre eux déclarant ne pas savoir à qui s'adresser ni où trouver de l'aide.[10] Une deuxième série d'entretiens approfondis avec plus de 100 jeunes survivants en Amérique latine, en Europe de l'Est et au Moyen-Orient a été réalisée en 2025, et les résultats seront bientôt disponibles.
- **Global Boys Initiative** documente les expériences de garçons victimes d'exploitation et d'abus sexuels dans dix pays, en mettant en évidence les obstacles à la divulgation, au signalement et à l'accès aux services.[148]
- **Notre** étude **« Male Survivors » (Survivants masculins)** fournit l'un des plus grands ensembles de données sur les garçons victimes d'abus sexuels. Elle met en évidence des schémas distincts, tels que des débuts précoces, des profils d'agresseurs différents et des délais plus longs avant la divulgation, soulignant la nécessité de mener des recherches et de fournir des services tenant compte des spécificités de chaque sexe.[114]
- **Secrets Worth Sharing** est une plateforme qui fournit des ressources tenant compte des traumatismes et reconnaissant la diversité des expériences des survivants. Elle propose des ateliers, des podcasts et des vidéos axés sur les survivants, couvrant des sujets tels que les abus sexuels sur les enfants, l'intersectionnalité dans les traumatismes et les enfants présentant des comportements sexuels nuisibles.[149] Comme l'a déclaré le fondateur :

> « Une chose que nous faisons différemment en tant qu'organisation est de produire des ressources en ligne spécifiques à différents facteurs d'identité, tels que le fait d>être un homme noir, ou queer, ou de parler une autre langue. Mon engagement le plus important auprès des adolescents et des jeunes concerne les suggestions pour ces épisodes [podcasts et vidéos]. Je pense que cela s'explique par le fait que les enfants et les jeunes ne veulent pas se considérer uniquement comme des survivants ou des victimes, mais s'intéressent à la manière dont leurs expériences sont uniques en fonction de leur propre identité. »
>
> *Société civile*[150]

Éducation et soutien communautaires

« Pour promouvoir l'éducation et la collaboration numériques, il ne faut pas se concentrer uniquement sur les outils de sécurité, mais aussi sur l'autonomisation des enfants et des adolescents en leur donnant les connaissances et les compétences nécessaires pour naviguer de manière sûre et responsable. Il faut impliquer les parents, les éducateurs et les jeunes eux-mêmes dans la création d'environnements numériques plus sûrs et plus positifs. »

Homme de 18 ans, Nicaragua[151]

Les efforts d'éducation et de sensibilisation doivent viser à modifier les comportements et à encourager le signalement et la recherche d'aide. Ils doivent être fondés sur des résultats scientifiques, adaptés au contexte, accessibles à tous les enfants et coordonnés entre les différents secteurs afin de garantir des rôles clairs et des messages cohérents et efficaces.

Les enfants ont besoin de multiples moyens fiables pour signaler leurs préoccupations, demander de l'aide et accéder à des services de soutien axés sur les survivants, notamment des lignes d'assistance téléphonique, des canaux de signalement officiels, des « pairs aidants » formés et des adultes de confiance.

Des interventions précoces et fondées sur des données probantes devraient être mises à la disposition des enfants exposés à des risques de préjudice, ainsi que des enfants et des adultes susceptibles de causer un préjudice.

Les messages de dissuasion et les avertissements devraient être adaptés aux différentes personnes susceptibles de causer un préjudice et s'accompagner de voies d'accès immédiates à un soutien pour les pensées et les comportements sexuels préjudiciables.

Campagnes d'éducation et de sensibilisation

« Nous devons éduquer à la fois les enfants et les parents sur la sécurité en ligne... J'ai l'impression que la plupart des gens pensent qu'ils n'ont nulle part où aller [pour obtenir de l'aide] parce que c'est en ligne... Les parents doivent également être mieux informés sur la manière de gérer ces situations. Et les lois pourraient être plus strictes, en particulier dans mon pays, je n'ai jamais beaucoup entendu parler de ce sujet. »

Jeune fille de 14 ans, Éthiopie[60]

Les initiatives d'éducation et de sensibilisation sont essentielles à la prévention. Ces efforts doivent aller au-delà de la simple sensibilisation pour susciter un véritable changement de comportement et garantir l'accès à l'aide.[9]

Des experts de tous les secteurs, ainsi que des défenseurs des jeunes et des survivants, ont souligné que pour être efficaces, les efforts d'éducation et de sensibilisation doivent :

- Être informés par les enfants et les survivants ou élaborées en collaboration avec eux, tenir compte des traumatismes et être adaptées au contexte.
- Éviter les messages fondés sur la peur ou la stigmatisation qui dissuadent de signaler les cas et de demander de l›aide.
- Être inclusifs et accessibles. Ils doivent être dispensés dans plusieurs langues, formats et lieux, y compris dans les écoles et autres espaces physiques et numériques où les enfants apprennent et interagissent. Des efforts doivent être faits pour atteindre les groupes marginalisés, notamment les enfants handicapés, les enfants non scolarisés et ceux vivant dans des zones rurales ou dans des contextes éducatifs fragiles.
- Doter les enfants et les adultes – y compris les personnes qui s'occupent d'eux, les éducateurs et les prestataires de services – des connaissances et des compétences nécessaires pour prévenir, reconnaître et réagir à l'exploitation et aux abus sexuels en ligne et hors ligne. Cela devrait inclure des informations sur les lois applicables, la manière de signaler les problèmes, les endroits où trouver de l'aide, la manière de soutenir les enfants et leurs pairs, et la manière d'éviter de causer du tort.
- Être coordonnés et durables, avec des rôles clairs pour les écoles, les familles, les communautés, l'industrie et le gouvernement afin de garantir la cohérence et l'efficacité des messages.
- Être adaptée à l'âge et au stade de développement des enfants et stratégiquement programmée (par exemple, avant qu'un enfant ne reçoive son premier téléphone ou ne commence à aller sur Internet sans surveillance).

Certaines victimes et certains défenseurs des jeunes ont exprimé leur inquiétude quant au fait que l'éducation pourrait avoir du mal à suivre le rythme des risques associés aux technologies en rapide évolution (par exemple, la réalité étendue) et que les établissements d'enseignement formel pourraient intimider les enfants ou ne pas leur sembler approprié pour discuter de questions sensibles. Cela souligne la nécessité d'impliquer les enfants dans l'identification des risques et l'élaboration des initiatives d'éducation et de sensibilisation.

« Beaucoup d'enfants ne voudront pas participer à quelque chose comme ça [l'éducation scolaire] parce que c'est... encore un sujet tabou et que certains enfants auront peur de s'exprimer et de parler. »

Survivante[77]

> « Les parents, en particulier les nouveaux arrivants, peuvent ne pas avoir les compétences linguistiques ou les connaissances technologiques nécessaires pour suivre [les risques associés aux nouvelles technologies]. Les ressources... devraient enseigner la sécurité sur les réseaux sociaux, ou les écoles devraient envoyer des documents en plusieurs langues pour informer les parents. »

Défenseur des droits des enfants, Canada[38]

Les programmes de prévention des abus sexuels sur les enfants sont bien étayés par des résultats scientifiques, mais les preuves concernant en particulier les programmes traitant des risques liés à la technologie sont encore limitées et en cours d'élaboration.

- **Le programme TOCSE (Tackling Online Child Sexual Exploitation)** lutte contre la violence en ligne au niveau individuel, communautaire, industriel et systémique au Vietnam. Il implique les enfants dans des consultations participatives, la conception de documents adaptés aux enfants et des initiatives menées par les enfants dans les écoles.[153,154] Le programme TOCSE a permis de dispenser une éducation et une formation professionnelle à plus de 18 000 enfants âgés de 12 ans et plus, ainsi qu'à 11 000 parents et enseignants, tout en renforçant les services d'assistance téléphonique et de soutien aux enfants.[153,154]
- Le rapport de l'UNICEF sur les programmes parentaux s'appuie sur une synthèse rapide des données disponibles et sur des consultations avec plus de 50 experts de divers secteurs afin d'identifier les éléments clés à prendre en compte pour concevoir des interventions qui aident les parents et les personnes qui s'occupent d'enfants à prévenir et à lutter contre la CSEA facilitée par la technologie.[155]

> « Je pense qu'il devrait y avoir davantage de cours et d'ateliers dans les écoles sur l'exploitation ou les abus sexuels des enfants en ligne... Je pense que j'aurais facilement pu en être victime. Mais maintenant que j'ai participé à quelques ateliers, je sais mieux comment les trafiquants s'y prennent pour victimiser les gens et comment ils choisissent leurs victimes... Je pense donc qu'éduquer les élèves sur la manière dont les victimes sont choisies par les trafiquants permettrait vraiment de les empêcher dêtre victimes de la traite. »

Défenseur des droits des enfants, Canada[38]

> « Il faut davantage sensibiliser les enfants à ce qu'il faut éviter et pourquoi il faut l'éviter. Les enfants n'écoutent pas lorsqu'on leur dit simplement de ne pas faire quelque chose. Il vaut mieux leur donner une éducation étape par étape et leur expliquer les aspects dérangeants de ce qui est mal afin qu'ils sachent qu'ils ne doivent pas le faire. »

Défenseur des droits des enfants, Kenya[38]

Des campagnes de sensibilisation efficaces peuvent modifier les comportements et renforcer l'idée que l'exploitation sexuelle des enfants est évitable. Elles peuvent également réduire la stigmatisation liée au signalement, à la recherche de justice et à la demande d'aide pour des pensées et des comportements sexuels préjudiciables. Par exemple, à la suite de la campagne de sensibilisation de l'Agence nationale britannique contre la criminalité (UK National Crime Agency) sur l'extorsion sexuelle , la proportion de personnes interrogées qui ont déclaré qu'elles partageraient des images explicites dans un scénario d'extorsion a considérablement diminué.[156] De même, les données de l'IWF montrent qu'après une campagne sur la diffusion non consensuelle d'images intimes, l'utilisation de l'outil **« Report Remove » (Signaler et supprimer)** a augmenté, même si la campagne ne faisait pas spécifiquement la promotion de cet outil.[157] Cependant, le contenu, la qualité et l'efficacité des campagnes varient, et peu d'initiatives font l'objet d'une évaluation formelle. Voici quelques exemples récents de campagnes de sensibilisation :

- **Help Children be Children** en Ouganda et en Zambie, qui combinent des campagnes de sensibilisation avec le renforcement des capacités des lignes d'assistance téléphonique et des forces de l'ordre. Ces campagnes ont permis d'augmenter le nombre de signalements et d'améliorer les connaissances du personnel des lignes d'assistance téléphonique.[157]
- **Beware the Share de l'ONUDC**, des campagnes interactives en langue locale ont informé le public sur le grooming, le sexting et les abus basés sur des images dans cinq pays d'Asie du Sud-Est.[158]
- En réponse à une étude révélant que 70 % des parents népalais ignoraient les risques et les dangers de l'exploitation sexuelle des enfants en ligne, ChildSafeNet s'est associé à TikTok pour dispenser une formation sur la sécurité numérique aux enfants, aux parents et aux éducateurs dans sept districts du Népal.[159]

> « Je pense que tout le monde devrait être sensibilisé dès son plus jeune âge à l'utilisation et à l'abus des technologies numériques, et à la manière de faire face à ces problèmes s'ils surviennent. Et dans les deux cas, la famille, les amis et chaque personne devraient en être conscients. »

Femme de 19 ans, Népal[38]

Comportement responsable envers les jeunes et les enfants (RBYC) : promouvoir le développement de normes sexuelles saines et lutter contre les abus commis par des pairs d'âge proche

Développé par des experts en prévention des abus sexuels sur les enfants et de la violence à l'école chez MOORE | Preventing Child Sexual Abuse, Johns Hopkins Bloomberg School of Public Health.

RBYC est un programme scolaire fondé sur des données probantes destiné aux 11-14 ans qui vise à prévenir les comportements sexuels problématiques et à aider les jeunes adolescents à développer des interactions sûres et appropriées – avec des enfants plus jeunes, leurs pairs et des adultes – tant en ligne que hors ligne.[74] Le programme se compose de cinq sessions interactives accompagnées de vidéos animées et de discussions en classe.[74]

Une grande partie des abus sexuels sur les enfants sont perpétrés par d'autres enfants et adolescents. Le début de l'adolescence est une étape cruciale du développement, au cours de laquelle les jeunes forment leur identité et leurs normes sexuelles et peuvent manquer des compétences ou des connaissances nécessaires pour gérer en toute sécurité les relations qui se nouent.[160,161] **Le programme RBYC** comble ces lacunes grâce à une approche tenant compte des traumatismes et axée sur les points forts. Le programme peut être dispensé de manière autonome ou intégré à des programmes existants en matière de santé, d'éducation sexuelle ou de prévention de la violence. Les sessions couvrent les thèmes suivants :

- Les relations saines et la prise de décision
- Les limites personnelles et le consentement
- Les différences de développement entre les adolescents et les enfants plus jeunes
- Les comportements responsables et irresponsables dans les contextes en ligne et hors ligne
- Identification et prévention des comportements sexuels problématiques
- Adultes et amis sûrs

Le programme RBYC comprend des documents à emporter à la maison pour les familles et des éléments destinés aux éducateurs et aux parents/tuteurs afin d'encourager une communication ouverte et de renforcer les messages de prévention à la maison et à l'école.

Un essai contrôlé randomisé mené auprès de 160 élèves aux États-Unis a révélé que les enfants qui ont participé au **programme RBYC** ont démontré une augmentation significative de leur capacité personnelle à prévenir les préjudices sexuels et une amélioration de leurs connaissances sur les différences de développement, le consentement et les comportements sexuels problématiques par rapport à ceux qui n'ont pas suivi le programme.

Au-delà de son essai aux États-Unis, **le programme RBYC** est en cours d'adaptation et de déploiement à l'échelle mondiale. Le programme a été adapté pour être utilisé en Allemagne (où un essai contrôlé randomisé est en cours dans 24 écoles) et aux Philippines (où il touche 250 élèves dans le cadre de programmes de prévention mixtes).[162] En collaboration avec le Kennedy Krieger Institute, **le programme RBYC** a également été adapté aux adolescents neurodivergents et enrichi de vidéos éducatives afin d'améliorer son accessibilité et son attractivité.[8]

Contenu sexuel autoproduit impliquant des enfants

> « Les enfants vont le faire [le sexting] dans le cadre de leurs relations, et comment faire pour qu'ils le fassent d'une manière qui ne leur portera pas préjudice ? »

Société civile[11]

Le partage d'images intimes peut être une partie normale des relations entre adolescents. Cependant, la distribution et la criminalisation de ce type de contenu peuvent causer des dommages, en particulier lorsque les lois et les politiques ne font pas la distinction entre le CSAM produit par des adultes et les images autoproduites impliquant des enfants. Les données montrent que les approches fondées sur la peur ou l'abstinence sont souvent inefficaces et peuvent décourager le signalement et la recherche d'aide.[163]

> « Il y avait un travailleur social et un policier qui nous en parlaient et disaient que... si vous envoyez vos propres photos nues, cela reste de la distribution de pornographie enfantine, donc... Je suis presque sûr que la moitié des personnes présentes avaient elles-mêmes envoyé des photos nues... Elles se disaient probablement : 'Oh, il y a un policier juste là et il va m'arrêter en plein milieu du gymnase.' »

Femme de 17 ans[164]

Leaked : Eclairage sur les contenus intimes et sexuels autoproduits par les jeunes en Thaïlande

- Les jeunes partagent et rencontrent couramment des contenus à caractère sexuel en ligne et décrivent principalement le préjudice comme survenant lorsqu'ils perdent le contrôle de ces contenus.
- Les approches fondées sur l'éducation sexuelle peuvent être plus efficaces que les avertissements sévères et les menaces contre tout partage de contenu à caractère sexuel.

Leaked est un partenariat de trois ans entre le projet HUG, une ONG basée à Chiang Mai, et le cabinet de recherche Evident, basé à Bangkok, soutenu par la World Childhood Foundation.[165,166,167] Cette initiative vise à mieux comprendre comment les jeunes en Thaïlande interagissent avec -et interprètent- les contenus intimes et sexuel autoproduits par les jeunes. Elle comprend une enquête représentative de la population menée auprès de 1 916 jeunes âgés de 9 à 17 ans dans des écoles du nord de la Thaïlande, ainsi que des entretiens approfondis avec des experts concernés. Les informations tirées des données permettront d'élaborer de nouveaux programmes éducatifs adaptés au cours de la dernière année du projet.[110]

Plus d'un jeune sur trois (36 %) déclare avoir reçu ou vu des images à caractère sexuel d'une personne supposée avoir moins de 18 ans. Les motivations supposée au partage de ce contenu à caractère sexuel sont variées. Beaucoup pensent que le contenu était partagé pour obtenir des likes et des followers (46 %), pour gagner de l'argent, des cadeaux ou des crédits (45 %), pour se sentir bien dans leur peau (40 %) ou pour montrer leur confiance dans une relation (27 %).[110] Un jeune a expliqué :

> « Certains de mes amis et connaissances plus jeunes ont également partagé des images de nudité. Lorsque je leur ai demandé quelles étaient leurs motivations, ils m'ont répondu qu'ils cherchaient à être acceptés. Ils avaient confiance en leur corps, mais n'avaient pas pleinement pris en compte les conséquences potentielles. Ces personnes sont talentueuses, mais elles manquent d'espace et d'opportunités pour s'exprimer. Elles se sont donc livrées à ce comportement afin d'attirer l'attention. »

Informateur clé âgé de 18 ans[110]

Une proportion notable de participants (34 %) pense que les jeunes partagent du contenu à caractère sexuel parce qu'ils sont soumis à des pressions, trompés ou contraints. Les jeunes dénoncent également la manière avec laquelle la technologie rend trop facile le partage impulsif d'images sexuellement explicites, tout en offrant peu de soutien lorsque des problèmes surviennent.[110]

Le projet **Leaked** souligne de manière cruciale que les préjudices identifiés par les jeunes ne découlent pas du partage de contenus intimes en soi, mais de la perte de contrôle sur ceux-ci. Le partage non désiré d'images à caractère sexuel produit par les jeunes eux-mêmes est apparu comme la principale préoccupation signalée par les jeunes (81 %), suivi par le regret (76 %), le harcèlement (70 %) et la détresse émotionnelle (68 %).[110] Ces données remettent en question les approches traditionnelles fondées sur la peur, qui reposent sur des avertissements sévères et des menaces juridiques pour décourager le partage de tout contenu à caractère sexuel. Ces messages ne reflètent pas la réalité de la vie des jeunes et peuvent en fait aggraver la stigmatisation ou les dissuader de demander de l'aide. Au contraire, les données du projet **Leaked** soutiennent une approche qui préconise :

- Une éducation sexuelle complète, fondée sur les droits, qui reconnaisse le rôle de la technologie dans les interactions sexuelles modernes
- Des fonctionnalités de sécurité renforcées sur les plateformes afin de protéger les enfants contre les contenus sexualisés, sensationnels ou préjudiciables
- Des changements culturels – passant de la punition au soutien – dans la réponse aux problèmes liés aux contenus à caractère sexuel générés par les utilisateurs
- Des espaces sans jugement pour un dialogue ouvert avec les jeunes sur la prise de décisions en ligne

> « Je pense que nous devrions simplement essayer de comprendre leur situation et ne pas blâmer les victimes. Comme c'est courant dans mon pays... Les gens se contentent de suivre le mouvement et d'insulter la personne qui était en fait la victime. »

Jeune homme de 17 ans, Pakistan[60]

Soutien aux adultes et aux enfants susceptibles de causer du tort

> « Appeler la ligne d'assistance pour la première fois a été la chose la plus difficile que j'ai jamais faite, mais je suis tellement content de l'avoir fait. [C'était la] première fois depuis des années que je reconnaissais ma dépendance à la pornographie adulte, qui m'avait conduit à regarder d'autres images [CSAM]. J'ai reçu un soutien formidable et je ne me suis jamais senti jugé. »

Appelant anonyme à **Stop It Now!**[112]

Les programmes de prévention de la perpétration constituent des stratégies de prévention importantes, étayées par des résultats de plus en plus nombreux.[28] Ils peuvent apporter une aide précoce aux personnes préoccupées par leurs propres pensées ou comportements sexuels envers les enfants, interrompre le processus menant à la perpétration d'infractions et prévenir les dommages avant qu'ils ne se produisent. Les pensées et comportements sexuels préjudiciables commencent souvent dès l'enfance, ce qui souligne la nécessité d'interventions précoces et adaptées à la fois pour les adultes et les enfants susceptibles de causer du tort.[168] Les obstacles à la recherche d'aide peuvent être réduits en proposant plusieurs options accessibles qui privilégient l'anonymat et fixent des limites claires en matière de confidentialité.[168] Voici quelques exemples d'initiatives de prévention des actes répréhensibles :

- Le projet **ReDirection** interroge des personnes anonymes qui recherchent du matériel d'abus sexuels d'enfants sur le dark web et les redirige vers des services d'aide, tout en générant des données qui permettent d'élaborer des stratégies de prévention efficaces.[169] Avec plus de 26 000 réponses recueillies en plusieurs langues, le projet a fourni des informations importantes sur les parcours des délinquants et leur comportement en matière de recherche d'aide. Le programme d'auto-assistance ReDirection a été évalué en termes d'évolutivité et fait actuellement l'objet d'une évaluation plus approfondie.
- **Help Wanted**, un cours en ligne destiné à aider les adolescents et les jeunes adultes attirés par les enfants plus jeunes, a été développé aux États-Unis et est actuellement adapté au Mexique et évalué.[170]
- La ligne d'assistance **Stop It Now!** fournit des conseils et un soutien confidentiel aux personnes préoccupées par leurs propres pensées ou comportements sexuels ou ceux d'autres personnes à l'égard des enfants. Le soutien est disponible dans plus de 200 langues. En 2023-2024, près de la moitié des 4 000 clients qui ont appelé la ligne d'assistance étaient des adultes cherchant de l'aide pour leurs propres pensées et comportements, y compris ceux qui avaient déjà fait du mal à des enfants.[112] Environ 12 % des personnes cherchant de l'aide étaient inconnues des autorités au moment du premier contact, ce qui suggère que les lignes d'assistance peuvent atteindre les personnes à risque avant que les forces de l'ordre n'interviennent.[112]
- **Prevention Global** est une plateforme de connaissances et une initiative de recherche ambitieuse qui évalue sept programmes développés pour prévenir les abus sexuels sur les enfants, notamment la thérapie individuelle et de groupe, le conseil à distance, les supports autoguidés et les programmes scolaires. **Prevention Global** publie également une série de produits de connaissances et la publication **Scalability** explore les obstacles et les opportunités pour étendre les programmes de prévention, y compris une évaluation des programmes axés en particulier sur la fourniture de services d'aide aux personnes en détresse.[125]

> « Nous constatons que certains délinquants peuvent être détournés de leur comportement délictueux. Si nous nous concentrions davantage sur cet aspect, nous ferions un meilleur travail. Mais c'est vraiment difficile à comprendre pour les gens...C'est un discours très compliqué à accepter sur le plan politique et social... ce qui le rend peu populaire à discuter et à financer. Mais il existe de plus en plus de preuves montrant que pour certaines [personnes], il est possible d'intervenir et de les détourner de la voie sur laquelle elles se trouvent. »

Société civile[11]

Dissuader la recherche de CSAM : les enseignements de la Lucy Faithfull Foundation

La Lucy Faithfull Foundation œuvre à la prévention des abus sexuels sur les enfants en proposant des services professionnels aux personnes susceptibles de commettre des abus, aux familles touchées par ces abus, ainsi que des outils et des ressources aux professionnels afin de créer des environnements plus sûrs pour les enfants.

- Les typologies et les parcours des délinquants varient considérablement, ce qui nécessite des tactiques adaptées et des messages diversifiés et multicanaux pour atteindre différents profils de délinquants.
- Des avertissements doivent être diffusés à chaque point où une personne pourrait tenter d'accéder à des contenus illégaux.
- Les messages doivent être neutres et soigneusement rédigés. Les messages de dissuasion ne suffisent pas à eux seuls à dissuader les délinquants, mais associés à une aide accessible et anonyme, ils peuvent encourager les personnes concernées à demander de l'aide pour gérer leurs pensées et leurs comportements sexuels.

> « La majorité du public préfère considérer les infractions sexuelles comme quelque chose qui 'concerne les autres'. C'est quelque chose qui arrive à d'autres personnes. Les autres sont les délinquants. Les autres sont les victimes... Cela ne contribue en rien à la protection des enfants. Cela ne contribue en rien à la sécurité des enfants... vous ne remarquerez pas si votre enfant abuse d'un autre enfant... vous ne le remarquerez pas si vous ne recherchez que des monstres et des prédateurs. »

Société civile[11]

La Lucy Faithfull Foundation a été la première à diffuser des messages de dissuasion par le biais de campagnes sur des canaux en ligne et hors ligne, notamment les médias d'information traditionnels, les réseaux sociaux, la publicité numérique payante, des courts métrages et des partenariats avec les forces de l'ordre et d'autres organisations statutaires et bénévoles[171]

Au cours de ses onze années de campagne de dissuasion, la Lucy Faithfull Foundation a identifié quatre messages clés qui avertissent efficacement ceux qui recherchent du matériel d'abus sexuels d'enfants :

- L'accès à des images à caractère sexuel mettant en scène des enfants est un crime.
- Cela cause du tort aux enfants.
- Cela a des conséquences pour vous et votre famille.
- Une aide anonyme est disponible si vous souhaitez arrêter.

La Lucy Faithfull Foundation, en partenariat avec l'IWF et Aylo (une plateforme de contenu pour adultes), a testé si des messages dissuasifs anonymes basés sur un chatbot pouvaient perturber et réduire les recherches de CSAM sur Pornhub UK. Aylo tient à jour une liste dynamique de milliers de termes interdits en raison de leur association avec des images sexuelles d'enfants. Lorsqu'un utilisateur recherche l'un de ces termes sur Pornhub UK, un message d'avertissement statique apparaît. De plus, un chatbot apparaît, ressemblant à une boîte de service client standard que l'on voit couramment sur d'autres sites web. En fonction des réponses des utilisateurs, le chatbot peut diriger les personnes vers des services d'aide anonymes, notamment la ligne d'assistance **Stop It Now !**, l'assistance par e-mail ou par chat en direct, des ressources d'auto-assistance en ligne, la ligne nationale de prévention du suicide ou les services d'urgence en santé mentale du service national de santé (National Health Service).

Une évaluation de l'intervention a révélé que :[171]

- 82 % des sessions de recherche de contenus illégaux ont été interrompues. Certains utilisateurs ont mis fin à leur session, tandis que d'autres sont passés à des contenus légaux ou ont quitté le site.
- La combinaison du message d'avertissement et du chatbot a efficacement encouragé les personnes à demander l'aide des services **Stop It Now!**
- Lorsque le chatbot a été désactivé pendant un mois, les recherches de CSAM ont augmenté.

Impact du projet en chiffres

- Une réduction statistiquement significative des recherches d'images à caractère sexuel mettant en scène des mineurs de moins de 18 ans a été observée au cours des 18 mois du projet.
- Le chatbot et le message d'avertissement ont été affichés 2,8 millions de fois.
- 99,8 % des recherches effectuées au cours des 18 mois du projet n'ont pas déclenché le chatbot ou le message d'avertissement.
- 1 656 personnes ont demandé des informations sur les services d'assistance téléphonique après avoir vu le chatbot ou le message d'avertissement.
- 490 personnes ont visité le site web **Stop It Now!** après avoir vu un message d'avertissement ou le chatbot.
- 68 personnes ayant appelé la ligne d'assistance **Stop It Now!** ont été identifiées comme ayant interagi avec le chatbot.

Options de signalement accessibles et fiables et soutien centré sur les survivants

> « Les gouvernements, les entreprises technologiques et les établissements d'enseignement devraient [...] veiller à ce que les enfants puissent signaler les cas où qu'ils se trouvent et à tout moment [...] afin que les mesures nécessaires puissent être prises pour contribuer à réduire ce phénomène. »

Femme de 24 ans, Ouganda[38]

Une gamme de mécanismes de signalement accessibles et fiables est nécessaire pour mettre en relation les enfants victimes de préjudices avec des services de soutien complets, adaptés aux enfants et axés sur les survivants. Les données montrent systématiquement que les enfants ont rarement recours aux canaux de signalement officiels. Par exemple, **Disrupting Harm** a mis à jour que seuls environ 3 % des enfants victimes d'exploitation ou d'abus sexuels en ligne ont signalé les faits à une ligne d'assistance ou à la police, contre 40 % qui en ont parlé à des amis et 24 % à des frères et sœurs.[60]

> « Je pense que beaucoup de gens ne parlent pas à leurs parents parce qu'ils ont peur qu'on leur interdise d'utiliser leur téléphone s'ils se confient... Beaucoup d'enfants peuvent se sentir coupables, surtout en cas d'abus sexuel. Ils peuvent se sentir coupables et penser que c'est aussi de leur faute. »

Jeune fille de 15 ans, Royaume-Uni[60]

> « Je ne parle généralement pas aux adultes. Je parle plutôt à des personnes de mon âge, car elles vivent des choses similaires et peuvent plus facilement comprendre ma situation. Je sais que les adultes ont de bonnes intentions, mais j'ai parfois l'impression qu'ils ne comprennent pas tout à fait ou qu'ils voient les choses différemment, et... il vaut mieux que je parle à des personnes de mon âge. »

Jeune fille de 15 ans, Éthiopie[60]

> « Je préfère parler aux adultes parce que je pense qu'ils ont plus d'idées... Les adultes à qui je parle m'écoutent bien, en particulier ma sœur. »

Fille de 17 ans, Nigeria[60]

Les défenseurs des jeunes soulignent que les dispositifs de signalement doivent être faciles d'accès et d'utilisation, exempts de stigmatisation et dignes de confiance.[60] Certains jeunes suggèrent des modèles dirigés par des pairs, tels que des adolescents formés qui peuvent répondre efficacement et orienter leurs pairs vers les services d'aide appropriés.[60] Voici d'autres exemples concrets :

- **Meri Trustline**, une ligne d'assistance téléphonique en Inde qui soutient les enfants, les femmes et les personnes issues de groupes marginalisés exposés à des risques en ligne.[172] Les signalements effectués via WhatsApp, par e-mail ou par téléphone sont reçus par des conseillers formés. La plateforme intègre également l'outil **« Report Remove »** de l'IWF, qui permet aux enfants de signaler des contenus en ligne et de demander leur suppression.[173]
- Des modèles de services multidisciplinaires centrés sur l'enfant pour les enfants victimes d'abus et d'exploitation sexuels, tels que **Barnahus** (Maison des enfants), qui fournit des services adaptés aux enfants et tenant compte des traumatismes, notamment des entretiens médico-légaux, des examens médicaux, des services thérapeutiques et un soutien aux victimes et à leur famille. **Les centres d'accueil uniques** en sont un autre exemple : ils fournissent une réponse immédiate aux situations de crise et des services de soutien aux femmes et aux enfants victimes de violence sexiste, en particulier dans les pays à faible et moyen revenu. Leurs services complets et regroupés en un seul lieu comprennent des services juridiques, des services sociaux et des services de conseil.[174] L'UNICEF examine comment ces modèles de prise en charge «peuvent aider les enfants victimes de CSEA facilitée par la technologie».[174] Des expériences documentées provenant des Philippines, d'Afrique du Sud, du Nigeria et de Bulgarie seront bientôt disponibles.[174]
- Les produits de connaissance de Prevention Global **destinés aux jeunes (Serving Youth)** comprennent un **guide pratique à l'intention des responsables** d'organisations de jeunesse qui met en évidence huit pratiques systématiques pour prévenir et lutter contre les abus sexuels sur les enfants.[175, 176] Les recherches montrent une diminution de plus de 20 % de la prévalence de la victimisation dans les organisations au service des jeunes qui ont mis en œuvre des stratégies de prévention des abus sexuels sur les enfants.[180]

« À mon avis, la meilleure façon de procéder serait de les écouter sans les juger, de croire ce qu'ils disent, de leur donner accès à des services de conseil ou d'aide, et de s'assurer qu'ils savent qu'ils ne sont pas seuls, car cela signifierait beaucoup pour eux... se sentir en sécurité, être écoutés, bénéficier d'un soutien pour se rétablir, et aussi s'assurer que les personnes qui ont commis ces actes soient tenues responsables. »

Jeune fille de 15 ans, Éthiopie[38]

Sécurité numérique

« Alors que nous continuons à élaborer ces mondes numériques, nous devons veiller à le faire en gardant à l'esprit la sécurité. Il ne s'agit pas seulement de donner aux jeunes accès à de nouvelles technologies sympas, mais aussi de nous donner les outils nécessaires pour nous protéger, de nous apprendre à reconnaître quand quelque chose ne va pas et de créer des espaces où nous pouvons profiter de tous les avantages de ces innovations sans les dangers qui les guettent. »

Défenseur des jeunes[1]

La sécurité, les droits et le bien-être des enfants doivent être une priorité à tous les niveaux de la culture d'entreprise, de la gouvernance et de la formation du personnel.

Les entreprises doivent intégrer des évaluations d'impact sur les droits des enfants, des mesures de diligence raisonnable en matière de sécurité des enfants et des caractéristiques de conception centrées sur les enfants dans tous les processus de développement.

Les entreprises doivent détecter et enrayer de manière proactive les contenus et les comportements préjudiciables, en plus de la modération réactive.

La transparence, la responsabilité et la collaboration intersectorielle sont essentielles pour renforcer les défenses mondiales contre l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie.

Promouvoir une culture industrielle axée sur la sécurité des enfants

La création d'un écosystème numérique plus sûr pour les enfants nécessite une culture industrielle qui donne la priorité aux droits, à la sécurité et au bien-être des enfants à tous les niveaux de la culture d'entreprise, de la gouvernance, de la prise de décision et de la formation du personnel. La sécurité des enfants doit être mise en avant comme une responsabilité professionnelle dès le stade de la formation, y compris dans les programmes d'études en informatique et les parcours d'embauche dans l'industrie.[32] Le personnel impliqué dans la conception, le développement et la fourniture de produits et services numériques doit recevoir une formation continue afin de reconnaître et d'atténuer les risques pour les enfants. La sécurité des enfants devrait également être intégrée dans les politiques et codes de conduite des entreprises en matière de protection. En 2024, le gouvernement cambodgien a formé 48 entreprises de technologie numérique aux directives industrielles relatives à la protection des enfants en ligne. Quatre de ces entreprises ont ensuite intégré la protection des enfants dans leurs politiques internes et élaboré un code de conduite en matière de protection des enfants à l'intention de leur personnel.[159]

Les modérateurs de contenu et les agents de sécurité numérique de première ligne, décrits comme les « agents de sécurité essentiels de l'internet », accomplissent un travail vital et difficile, mais sont souvent confrontés à des conditions précaires et à des risques pour leur propre santé et leur bien-être. Ils devraient bénéficier de conditions d'emploi équitables, d'un développement professionnel, d'un accès à des services de santé mentale et de soutien psychosocial, ainsi que d'un soutien après

la fin de leur contrat.[181] De telles mesures peuvent améliorer la fidélisation du personnel, renforcer l'expertise et améliorer la qualité et l'efficacité des interventions de première ligne en matière de sécurité numérique.

Faire de la sécurité dès la conception la norme

Une approche axée sur la sécurité dès la conception (en anglais, Safety by Design) exige que toutes les parties prenantes impliquées dans la conception et le développement de produits et services numériques se posent la question suivante : « Que ferions-nous différemment si nous savions que l'utilisateur final est un enfant ? »[182] Elle transfère la responsabilité aux entreprises de veiller à ce que leurs produits ne causent pas de préjudice aux enfants. Ces mesures de sécurité doivent s'appliquer à toutes les technologies numériques, car les enfants accèdent souvent à des produits et services qui n'ont pas été spécialement conçus pour eux.[183] Plusieurs experts de la société civile ont fait remarquer que les intérêts commerciaux semblaient primer sur les droits et la sécurité des enfants.[184] Les représentants de l'industrie affirment qu'une approche axée sur la sécurité dès la conception n'est pas nécessairement en contradiction avec les intérêts commerciaux.

Les principales caractéristiques de la sécurité dès la conception sont les suivantes :[31]

- Intégrer systématiquement d'une par des évaluations pour comprendre l'impact sur les droits de l'enfant et d'autre part des mécanismes de vigilance dans les processus de conception et de développement. Les évaluations d'impact sur les droits de l'enfant sont des processus qui permettent aux entreprises d'évaluer comment leurs activités, leurs produits et leurs services affectent les droits des enfants, tels que définis dans la Convention des Nations unies relative aux droits de l'enfant et d'autres instruments relatifs aux droits humains.[185]
- Confidentialité et protection des données, y compris des paramètres de confidentialité stricts par défaut, des expériences utilisateur adaptées à l'âge et des mesures de protection contre l'utilisation abusive des données personnelles des enfants.
- Conception et éducation centrées sur l'enfant, par exemple en impliquant les enfants et les jeunes dans la conception et le test des produits, en fournissant des informations claires et accessibles et en intégrant des fonctionnalités éducatives qui renforcent l'autonomie et la sensibilisation des enfants.
- Protections intégrées telles que le contrôle parental, les limites de contact, les mesures de protection financière pour empêcher les enfants de transférer de l'argent en ligne et les modes ou appareils à fonctionnalités limitées.
- Redevabilité grâce à des obligations claires en matière de transparence, une modération rigoureuse et des mécanismes de signalement et de recours accessibles.

Les mesures de sécurité destinées aux enfants doivent être fonctionnelles, accessibles et disponibles de manière équitable dans toutes les régions géographiques et toutes les langues dans lesquelles un produit ou un service est proposé.

« Si vous ouvrez un compte [sur les réseaux sociaux] ici en Amérique latine et dans les pays du Sud, la question était de savoir s'ils bénéficieraient du même type de protections et de garanties que les personnes qui ont un compte aux États-Unis et au Royaume-Uni, et la réponse était : absolument pas !... Les gens ici en Amérique latine sont moins en sécurité que les enfants dans d'autres pays. Et pourquoi cela doit-il être ainsi ? »

Un cadre complémentaire, les droits de l'enfant dès la conception (*Child Rights by design*), reconnaît que les technologies numériques doivent soutenir la réalisation des droits des enfants, y compris leur droit à la sécurité.[186] La mise en œuvre de ces approches nécessite l'engagement des dirigeants, des ressources dédiées et du personnel formé. Les petites entreprises et les start-ups manquent souvent de ces capacités, mais des conseils sont disponibles pour aider les entreprises à évaluer l'impact des technologies numériques, y compris l'IA générative, sur les droits de l'enfant.[36,184,187–189] La mise en œuvre efficace des principes de sécurité dès la conception doit s'appuyer sur des données probantes et nécessite la transparence de l'industrie et des mécanismes de responsabilité indépendants.

Tableau 1. Exemples de sécurité dès la conception et de droits de l'enfant dès la conception dans la pratique

Élément de conception	Action	Exemples dans la pratique
Dispositifs de sécurité intégrés aux produits	Intégrer les évaluations des risques pour la sécurité dans le développement des produits.	**La boîte à outils D-CRIA** de l'UNICEF aide les entreprises à mener des évaluations d'impact solides sur les droits de l'enfant et à respecter leur devoir de vigilance en matière d'environnement numérique. Elle comprend un modèle D-CRIA, un guide de démarrage rapide et des conseils spécifiques pour la participation et l'engagement des enfants.[185] **Le cadre d'IA responsable et la liste de contrôle « Safety by Design »** de Thorn pour les plateformes technologiques visent à réduire les risques associés à l'IA générative.[188]
Dispositifs de sécurité intégrés aux produits	Concevoir des appareils ou des modes sécurisés pour les enfants, avec des fonctionnalités ou un accès limité. Les fonctionnalités avancées peuvent être débloquées par un parent ou un tuteur.	**HMD Fuse** est un smartphone sécurisé pour les enfants, doté d'un filtre de contenu IA intégré qui empêche la visualisation, l'enregistrement ou le stockage de contenus pornographiques. Il démarre en mode restreint, sans accès aux applications ni aux réseaux sociaux, à moins que les tuteurs n'activent des fonctionnalités supplémentaires.[190] **La sécurité des communications** Apple (Apple Communication Safety) est activée par défaut pour les comptes enfants. Elle analyse les images et les vidéos sur l'appareil afin de détecter et de flouter automatiquement les contenus à caractère sexuel, avertit l'enfant, fournit des conseils et des ressources de sécurité adaptés à son âge et permet le contrôle parental via les paramètres Screen Time (temps d'écran).[191]
Confidentialité et protection des données	Appliquer des paramètres par défaut et des mesures de protection stricts en matière de confidentialité, et collecter un minimum de données à partir des comptes enfants ou lorsque l'âge de l'utilisateur est incertain.	Les comptes d'adolescents sur les réseaux sociaux, **tels que le mode Snapchat Teen**, peuvent rendre les comptes privés, restreindre les messages directs, filtrer les contenus préjudiciables et désactiver le partage de localisation par défaut.[192] **YouTube Kids**, destiné aux enfants de moins de 13 ans, filtre les contenus, désactive les commentaires, le partage de localisation et les publicités personnalisées par défaut.

Élément de conception	Action	Exemples dans la pratique
Communication, éducation et mécanismes de signalement adaptés aux enfants	Fournir des informations, une éducation et des mécanismes de signalement/plainte adaptés à l'âge et aux enfants.	Le programme de sécurité numérique « **Be Internet Awesome** » de Google comprend des jeux interactifs sur la sécurité en ligne, la confidentialité et le partage respectueux.[193] LEGO a élaboré un code de conduite adapté aux enfants. L'application LEGO Life, aujourd'hui disparue, intégrait un outil appelé « **Captain Safety** » qui comprenait un engagement en matière de sécurité, des rappels de sécurité dans l'application et des explications adaptées aux enfants sur les politiques de confidentialité et de modération de LEGO.[194] Le programme de **partenariat scolaire** d'Instagram propose des ressources sur la sécurité numérique et donne la priorité aux signalements de contenus et de comptes préjudiciables soumis par les élèves et les enseignants, en garantissant leur examen dans les 48 heures.[195]

> « Quand elle était adolescente, elle cherchait une raison de dire non. Et il continuait à faire pression sur elle [pour qu'elle envoie davantage d'images à caractère sexuel], et elle ne pouvait pas se défendre… Elle ne pouvait pas dire non… Mais 'mon téléphone ne me permet pas de prendre des photos nues' semble être un moyen très efficace de redonner à ces victimes le pouvoir de dire qu'elles ne peuvent pas. 'Oui. Pas moi, l'appareil ne me le permet pas.' »
>
> *Société civile*[11]

Détecter et bloquer de manière proactive les contenus préjudiciables

Les entreprises technologiques devraient détecter et bloquer de manière proactive les contenus, comptes et comportements préjudiciables en temps réel à l'aide d'outils tels que les systèmes de correspondance de hachage et les filtres de surveillance des contenus, tout en respectant les droits des utilisateurs.[73]
Des efforts visant à exploiter l'IA et l'apprentissage automatique (machine learning) à des fins de détection proactive de contenus émergent. Parmi eux un service de détection du grooming qui utilise l'apprentissage automatique et un système intelligent de détection des CSAM qui permet de distinguer avec précision les publications CSAM et non CSAM sur le dark web tout en générant des informations exploitables sur les créateurs et les victimes.[196,197] Le produit **Safer** de Thorn est une suite d'outils basés sur l'IA que les entreprises peuvent utiliser pour détecter, identifier et signaler les CSAM. **Safer** a été intégré à l'application web d'IA générative DALL-E2 d'OpenAI.[198]

La Tech Coalition teste actuellement un prototype permettant de détecter et de lutter contre la CSEA facilitée par la technologie dans les environnements de streaming en direct.[199] Ce projet pilote utilisera des signaux métadonnées, tels que les caractéristiques de la session et l'utilisation de services d'anonymisation, afin de générer un score de risque indiquant la probabilité que des abus sexuels commis sur des enfants en ligne se produisent au cours d'une session de streaming en direct donnée, afin que les équipes chargées de la sécurité des enfants puissent mener une enquête plus approfondie. Des tests et des évaluations auront lieu au printemps afin d'évaluer la faisabilité d'une adoption plus large par l'industrie.

Les enfants doivent pouvoir signaler immédiatement leurs préoccupations et les contenus et comportements préjudiciables qu'ils rencontrent en ligne — notamment le CSAM, l'extorsion sexuelle, le grooming ou la diffusion non consensuelle d'images — par le biais de canaux simples, fiables et intégrés à la plateforme.[60] Les signalements doivent donner lieu à des réponses rapides afin de supprimer les contenus et de bloquer les comptes préjudiciables, ainsi que de mettre les utilisateurs en relation avec des services d'assistance et d'assurer un suivi.

De nombreux produits numériques n'offrent pas de mécanismes de signalement accessibles, et même lorsqu'ils sont disponibles, les enfants ne les utilisent souvent pas. Une étude mondiale sur l'extorsion sexuelle a révélé que **seuls 4 % des enfants signalaient les incidents à la plateforme sur laquelle ils se produisaient.**[52] Les défenseurs des jeunes ont souligné que l'expérience du signalement et de la demande de retrait d'images à caractère sexuel est aussi importante que la fonction elle-même : elle doit être facile, sûre et exempte de stigmatisation. À titre d'exemple positif, le service **Take It Down** du NCMEC rassure les enfants grâce à des messages non stigmatisants (« avoir des photos nues en ligne est effrayant, mais il existe des moyens pour les faire retirer »), une assistance multilingue, des vidéos explicatives et des FAQ.[200] Les lignes directrices de l'OCDE (Organisation de coopération et de développement économiques) soulignent que les systèmes de recours doivent être conçus avec la participation des enfants et adaptés aux risques spécifiques à chaque plateforme.[182]

> « Je pense que [certaines plateformes numériques]... se concentrent davantage sur leurs profits que sur la sécurité [des enfants]. Une chose qui pourrait vraiment aider serait d'améliorer les mécanismes de signalement sur la plateforme, car je pense que la plupart du temps, il est très difficile de trouver où signaler un problème, et il n'y a pas beaucoup d'informations sur la façon dont cela fonctionne réellement. Et la plupart du temps, on n'a pas vraiment de réponse de leur part. On a donc l'impression que c'est sans espoir et que cela ne sert à rien de signaler quoi que ce soit. »
>
> *Jeune fille de 15 ans, Royaume-Uni*[60]

Transparence et responsabilité

Il est essentiel de renforcer les engagements en matière de transparence et prise de responsabilité. Les entreprises devraient mener des évaluations obligatoires de l'impact sur les droits des enfants et publier en temps utile des rapports de transparence qui recensent les risques, les préjudices et les comportements des utilisateurs afin d'éclairer les stratégies de prévention. Ces rapports pourraient par exemple inclure des données démographiques sur les victimes et les auteurs, les taux d'abandon de session ou les clics vers les services d'aide déclenchés par des fenêtres d'avertissement. La normalisation des indicateurs de sécurité des enfants et des processus de signalement dans l'ensemble du secteur pourrait permettre de relever les défis actuels en matière de comparabilité des données. Le programme **Lantern** de la Tech Coalition souligne la nécessité d'un écosystème où les données, les informations et les responsabilités sont partagées entre les différents secteurs afin de renforcer la protection des enfants en ligne.

Lantern – action coordonnée de l'industrie contre l'exploitation sexuelle des enfants en ligne : perspectives de la Tech Coalition

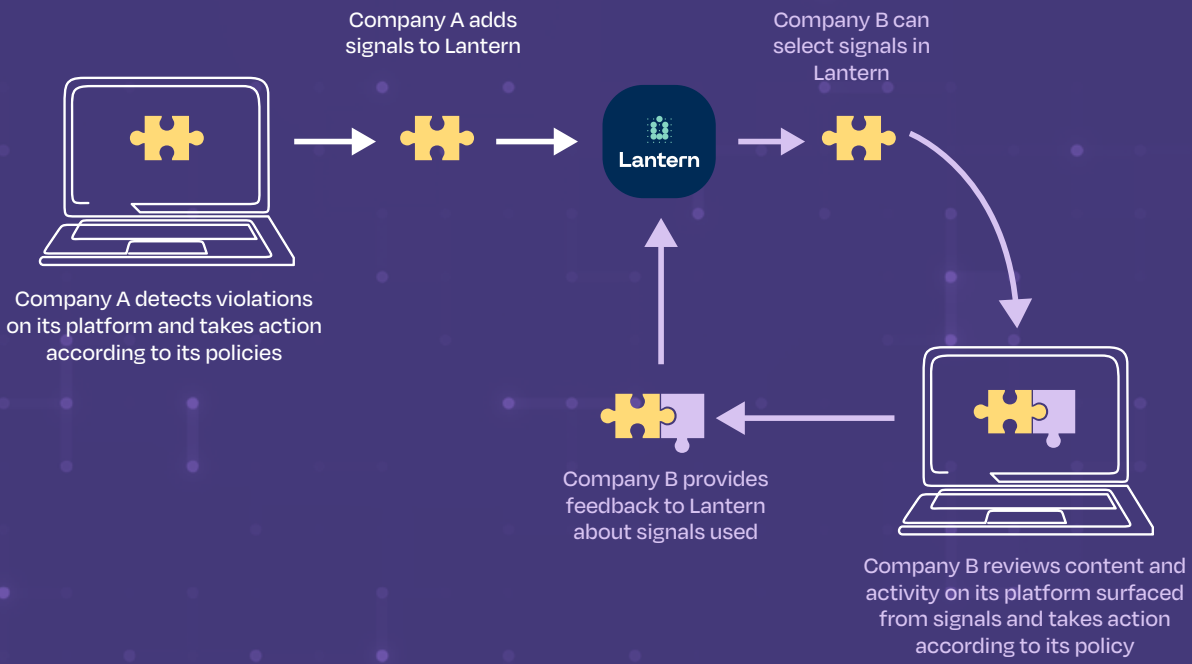
La Tech Coalition est une alliance mondiale regroupant plus de 55 entreprises technologiques qui s'engagent à protéger les enfants contre l'exploitation et les abus sexuels en ligne en partageant leurs connaissances, en identifiant les menaces et en développant des solutions collaboratives.

Les auteurs utilisent souvent plusieurs plateformes pour partager des contenus abusifs et exploiter les enfants en ligne. Historiquement, il n'existait pas de cadre universel pour coordonner les efforts de l'industrie visant à détecter l'exploitation et les abus, ce qui laissait des lacunes dans la détection et la réponse. **Lantern** a été créé pour combler cette lacune en permettant aux entreprises participantes de partager des signaux d'abus exploitables, ce qui permet de détecter et de répondre à des préjudices qui, autrement, pourraient passer inaperçus.[201]

Partant du principe que le partage des informations sur les menaces améliore la réponse de l'industrie à la CSEA en ligne, **Lantern** facilite la collaboration afin de renforcer les défenses collectives contre les menaces émergentes. Les signaux – tels que les hachages, les URL ou les noms d'utilisateur – représentent des contenus ou des comportements potentiellement préjudiciables liés à la CSEA en ligne. Lorsqu'une plateforme rend publique ces signaux, les autres peuvent examiner de manière indépendante les activités connexes sur leurs propres services.[25]

Lorsqu'une entreprise identifie des CSEA sur sa plateforme, elle prend les mesures appropriées pour faire respecter ses politiques de sécurité des enfants et partage les signaux associés via **Lantern**. Cela permet aux autres plateformes de détecter et de supprimer de manière proactive les contenus ou comptes concernés, renforçant ainsi l'écosystème global de sécurité en ligne.

Figure 6. Cadre et processus de partage des signaux **de Lantern**[25]



La collaboration via **Lantern** porte déjà ses fruits, les entreprises participantes constatant une amélioration constante de leur capacité à réduire les risques liés à la sécurité des enfants.[201] En 2024 :

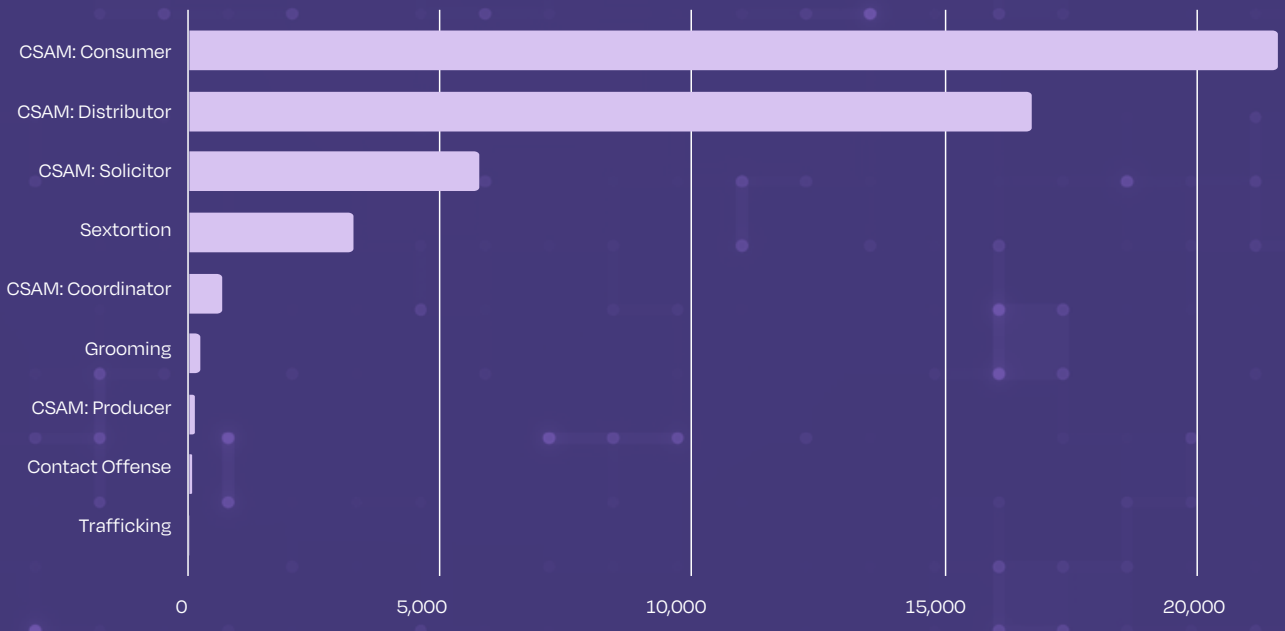
- Près de 300 000 nouveaux signaux de CSEA liés à Internet ont été partagés, portant le total à plus d'un million de signaux **Lantern** à ce jour.
- Plus de 100 000 comptes ont fait l'objet de sanctions pour des violations liées à l'exploitation et aux abus sexuels d'enfants.

- Plus de 135 000 URL hébergeant ou transmettant du CSEA ont été bloquées ou supprimées.
- Plus de 7 000 éléments de CSAM ont été supprimés.
- Des cas à haut risque, dont 81 incidents d'agressions sexuelles avec contact et 45 cas liés à la traite, ont été signalés.

La plupart des signaux liés à des incidents concernaient des auteurs cherchant à distribuer ou à obtenir du matériel d'abus sexuels d'enfants, parfois en prélude à un grooming ou à des abus avec contact.201 La taxonomie des signaux de Lantern permet une catégorisation plus précise des menaces, favorisant ainsi de multiples approches en matière de détection et de réponse.[201]

Figure 7. Signaux téléchargés par type en 2024

Figure 8. Catégories de signaux basés sur des incidents signalés en 2024



Lantern démontre la puissance de la collaboration intersectorielle dans la lutte contre l'exploitation et les abus des enfants en ligne. En brisant les silos entre les plateformes, le programme a amélioré la détection, la responsabilisation des auteurs et la rapidité de la réponse. Il démontre également de manière importante comment le partage de signaux liés au contenu et au comportement peut renforcer les défenses contre des menaces plus larges telles que le grooming, l'extorsion et la traite, en plus de la distribution de CSAM.

> « Ce qui m'a vraiment marqué, c'est l'importance du travail collectif... tout le monde doit s'impliquer dans la prévention. »
>
> *Industrie*[7]

Droit, politique et justice

> « Je pense que nous avons besoin de plus de réglementation, de législation. Et je pense qu'il en va de même pour le tabagisme et la toxicomanie. Nous ne laissons pas les enfants fumer. Nous ne laissons pas les enfants boire. Nous avons une législation. Il nous a fallu trop de temps pour réglementer Internet. »
>
> *Société civile*[11]

L'harmonisation de la législation est essentielle pour combler les lacunes juridiques, garantir la coopération transfrontalière et suivre le rythme des nouvelles menaces numériques.

La mise en œuvre efficace des lois dépend de systèmes judiciaires dotés de ressources suffisantes, sensibilisés aux traumatismes et centrés sur les victimes, qui protègent les enfants et ne les traumatisent pas à nouveau.

La lutte contre l'exploitation sexuelle des enfants à des fins commerciales facilitée par la technologie nécessite une action collaborative entre les gouvernements, les régulateurs, l'industrie et la société civile afin de tenir les responsables pour redevables.

Harmoniser la législation à l'échelle mondiale conformément aux normes relatives aux droits de l'enfant

Les efforts visant à harmoniser les législations nationales relatives à l'exploitation sexuelle des enfants à l'aide de technologies prennent de l'ampleur à l'échelle mondiale. La **Convention des Nations unies contre la cybercriminalité** est un traité multilatéral historique qui fait progresser les efforts visant à normaliser les lois mondiales en matière de protection des enfants, notamment en criminalisant pour la première fois à l'échelle mondiale la possession de CSAM et le grooming.[23] Des lois exhaustives telles que la **loi britannique sur la sécurité en ligne** *(Online Safety Act)* contribuent à réduire les incohérences qui existent naturellement lorsque les ministères et les domaines concernés légifèrent.[8,202] La récente politique globale de protection de l'enfance des Fidji, promulguée en 2025, a harmonisé **la loi** précédente **de 2024 sur les soins et la protection** et la **loi de 2024 sur la justice pour mineurs.** Elle visait également à réduire les lacunes et à améliorer la coordination entre les secteurs.[203] Cependant, à l'échelle mondiale, des incohérences persistent dans les efforts législatifs tant au sein des gouvernements qu'entre eux. L'absence d'un système centralisé permettant de suivre l'évolution de la législation et de partager les avancées ne fait qu'aggraver le problème mondial de l'incohérence législative. Des outils comparatifs tels que le **tableau de bord #BeBrave G7 Country Scorecard** du Brave Movement et **l'indice Online Safety Regulatory Index** mettent en évidence les progrès et les lacunes.[204,205]

> « Une grande partie [de l'extorsion sexuelle] provient de pays étrangers... mais chacun a ses propres juridictions et lois, et personne ne veut coopérer [de sorte qu'il] nous est très difficile de dire : Ne faites pas cela aux enfants. »
>
> *Survivante* [77]

Les progrès du Brésil en matière de protection des enfants en ligne en 2025

En 2025, le Brésil a franchi une étape importante dans la protection numérique des enfants grâce à des mesures politiques qui reflètent le leadership croissant des pays de la majorité mondiale dans la création d'environnements en ligne plus sûrs. En septembre, le Brésil a promulgué une loi complète qui impose aux entreprises et aux plateformes des obligations claires en matière de prévention, de détection et de réponse à l'exploitation sexuelle des enfants en ligne.19 La loi introduit une obligation de prévention, exige le retrait rapide des contenus illégaux sans attendre une décision judiciaire et impose le signalement aux autorités nationales. La loi intègre également les principes de sécurité et de confidentialité dès la conception, interdit la publicité ciblée destinée aux enfants et établit des règles strictes de vérification de l'âge, notamment le lien avec le compte parental pour les utilisateurs de moins de 16 ans. Les plateformes doivent fournir des outils de contrôle parental en portugais, publier des rapports de transparence et permettre l'accès à la recherche sur les données relatives au bien-être numérique des enfants. L'application de la loi sera assurée par l'Agence nationale brésilienne de protection des données.[19]

Des consultations multisectorielles, notamment avec l'industrie et les organisations de défense des droits de l'enfant, sont essentielles pour garantir que les lois suivent le rythme des menaces technologiques émergentes et s'alignent sur les normes en matière de droits de l'enfant, tout en permettant l'innovation qui renforce la sécurité des enfants. Les opinions sur la meilleure façon de protéger les enfants par le biais de la législation restent partagées. Parmi les personnes interrogées, un expert du secteur a plaidé en faveur de « zones de sécurité » législatives (avec des garanties strictes) pour tester et mettre à l'épreuve les outils de détection, tandis qu'un représentant de la société civile a averti que certaines lois sur le signalement obligatoire peuvent involontairement restreindre le signalement volontaire et rapide.[7]

La vérification de l'âge à l'ère numérique : trouver un équilibre entre protection et participation

- La vérification de l'âge désigne les méthodes utilisées pour vérifier ou estimer l'âge d'un utilisateur en ligne afin de garantir l'accès à des contenus adaptés à son âge. Ces méthodes impliquent des compromis entre précision, confidentialité et équité.
- Les lois récentes exigeant la vérification de l'âge ont attiré l'attention du public sur les risques liés à la sécurité des enfants en ligne et ont fait apparaître toute une série de défis éthiques, pratiques et politiques. Elles peuvent avoir des conséquences imprévues, telles que le contournement des restrictions par les utilisateurs ou l'exclusion de groupes marginalisés.
- La vérification de l'âge peut renforcer la sécurité des enfants en ligne, mais sans consultation significative des enfants et des jeunes, sa mise en œuvre risque de porter atteinte à leurs droits.
- Les restrictions d'âge ne doivent pas réduire l'importance des interventions familiales, scolaires et communautaires, ni minimiser l'importance de la responsabilité des entreprises et des évaluations d'impact sur les droits des enfants en relation avec les environnements numériques.

Tendances législatives mondiales

Depuis la dernière évaluation mondiale des menaces, de nombreux pays ont adopté des lois sur la vérification de l'âge et la sécurité en ligne :[206]

- Brésil : adoption d'une législation comprenant des obligations complètes de vérification de l'âge en septembre 2025.[19]
- Royaume-Uni : obligation pour les plateformes d'empêcher les jeunes d'accéder à des contenus préjudiciables, notamment par le recours à des systèmes de vérification de l'âge « hautement efficaces » (par exemple, estimation de l'âge à partir d'une pièce d'identité ou d'une photo) sur les sites pornographiques et les grandes plateformes de réseaux sociaux, à compter de juillet 2025.[202]
- Australie : restreindra l'accès des enfants de moins de 16 ans aux réseaux sociaux à partir de décembre 2025.[207]
- Singapour : exigera une vérification de l'âge dans les boutiques d'applications pour les téléchargements depuis Google Play, Apple et Huawei.[21]

D'autres pays ont envisagé ou récemment adopté une législation similaire, notamment le Danemark, la Malaisie, la Mongolie, la Nouvelle-Zélande, la Corée du Sud, la Turquie, l'Union européenne et l'Ouzbékistan.[50,51]

> « Beaucoup de lois élaborées pour les jeunes ne sont pas [vraiment] élaborées pour les jeunes . Par exemple, les interdictions actuelles d'accès aux réseaux sociaux pour les moins de 16 ans – les jeunes n'ont pas été suffisamment consultés. Les jeunes devraient être présents dans la salle lorsque les lois sont élaborées et développées, et pas seulement au stade de la consultation. »

Femme de 22 ans, Australie[38]

Le point de vue des enfants

Les enfants et les jeunes reconnaissent l'intérêt des lois sur la sécurité en ligne, tout en soulignant la nécessité de nuancer leur conception et leur mise en œuvre. Une enquête représentative à l'échelle nationale menée auprès d'enfants âgés de 8 à 17 ans en Australie a révélé que près de 90 % d'entre eux étaient favorables à la vérification de l'âge pour accéder à certains sites web, tandis que 56 % des adolescents américains interrogés soutenaient l'obligation de vérifier l'âge sur les réseaux sociaux.[208,209] Cependant, les jeunes soulignent également leurs préoccupations en matière de confidentialité, de sécurité et d'inclusion numérique.

> « Si vous voulez être protégé, vous devez faire quelques sacrifices en matière de liberté. Mais en tant que jeune, j'ai aussi le droit d'explorer et de découvrir des choses [dans le monde numérique]. »

Jeune[38]

Les détracteurs des interdictions générales avertissent que restreindre l'accès peut exclure ou isoler les jeunes marginalisés, tels que les minorités sexuelles et de genre ou les enfants sans papiers, et les pousser vers des espaces numériques non réglementés.[210] Des données provenant du Royaume-Uni montrent que l'utilisation des VPN a explosé après la mise en place de restrictions, soulignant les défis liés à l'application de la loi dans un monde connecté numériquement.[211]

> « Lorsqu'un enfant a besoin d'accéder à des plateformes de streaming mais ne dispose pas d'un compte, il utilise des sites illégaux qui affichent des publicités pop-up inappropriées au contenu explicite. »

Défenseur des droits des enfants, Kenya[38]

> « Les comptes alternatifs constituent un problème majeur. Si quelqu'un est banni, il peut créer un nouveau compte. Il existe tellement de façons différentes de contourner les interdictions ou les modérations. »

Jeune fille de 13 ans, Australie[38]

Équilibre entre sécurité, vie privée et droits

Les défenseurs affirment que « la vérification de l'âge ne devrait pas viser à exclure les enfants, mais à leur permettre d'accéder à Internet en toute sécurité ».[186] La politique de l'Union africaine en matière de sécurité et d'autonomisation des enfants en ligne (2024) adopte cette approche fondée sur les droits, favorisant l'accès parallèlement à la prévention.[212]

> « La vérification de l'âge est un outil, et non une fin en soi, pour offrir aux jeunes une expérience positive en ligne. Dans le meilleur des cas, elle protège ; dans le pire des cas, elle empêche les jeunes d'accéder à des informations, à des moyens d'expression et à des relations essentielles. »

Régulateur[206]

Tableau 2. Méthodes de vérification de l'âge[213]

Méthode	Description	Principales préoccupations
Auto-déclaration	L'utilisateur saisit sa date de naissance ou coche une case.	Facile à mettre en œuvre, mais peu fiable.[214]
Estimation de l'âge	Prédit l'âge à l'aide d'algorithmes ou de données biométriques.	Pratique, mais sujet aux biais et aux erreurs : des études montrent des taux d'erreur allant de 34 à 73 % chez les adolescents et des biais raciaux.[207,215]
Vérification de l'âge	Nécessite une pièce d'identité officielle ou un signal vérifié.	Méthode la plus précise, mais soulève des questions en matière de confidentialité, de sécurité et d'exclusion, en particulier pour les personnes ne disposant pas d'une pièce d'identité officielle.[216]

Il n'existe pas encore de norme mondiale pour la vérification de l'âge. Meta a proposé des vérifications sur les appareils ou dans les boutiques d'applications, tandis que Google explore des preuves à divulgation nulle de connaissance qui confirment l'éligibilité sans révéler l'identité. Les décideurs politiques et les entreprises doivent veiller à ce que les systèmes soient transparents, respectueux des droits, préservant la vie privée, équitables et conçus en collaboration avec les enfants.

Renforcement des capacités, réponse adaptée aux enfants et justice centrée sur les survivants

Les lois visant à protéger les enfants doivent s'accompagner d'investissements dans la formation, le renforcement des capacités et la mise en place d'autorités de régulation dédiées. Les gouvernements doivent veiller à ce que les forces de l'ordre, les procureurs et les magistrats reçoivent une formation continue sur les approches adaptées aux enfants et tenant compte des traumatismes, et disposent des ressources nécessaires pour les appliquer efficacement. Les victimes de toutes les régions signalent que les protections législatives existantes sont insuffisantes ou mal appliquées et réclament une justice centrée sur les victimes.[60]

> « Si vous portez plainte à la police... ils se moqueront de vous. C'est pourquoi nous avons besoin d'unités spécialisées dans la cybercriminalité. »
>
> *Défenseur des survivants*[60]

Au Kenya, le Conseil national sur l'administration de la justice a lancé un manuel de formation spécialisé à l'intention des acteurs du secteur judiciaire sur les enquêtes et les poursuites relatives aux abus sexuels commis sur des enfants à l'aide de technologies.[217] Cette initiative reflète la reconnaissance de la nécessité de mettre en place des pratiques adaptées aux enfants et tenant compte des traumatismes subis au sein du système judiciaire, allant au-delà de la législation pour soutenir des réponses efficaces centrées sur les survivants.

> « Les systèmes juridiques devraient leur permettre de signaler facilement les abus sans crainte, et les plateformes en ligne devraient agir rapidement pour supprimer tout contenu préjudiciable. »
>
> *Garçon de 15 ans, Éthiopie*[60]

Une détection proactive, indépendante des plaintes des survivants, est cruciale. Des outils tels que le classificateur CSAM de Thorn (via INTERPOL) et le logiciel résumant les vidéos alimenté par l'IA de Rigr AI améliorent la réactivité face aux cas de CSEA diffusés en direct.[218,219]

Les forces de l'ordre soulignent régulièrement que davantage de ressources sont nécessaires pour traiter le nombre croissant de signalements reçus par les lignes d'assistance téléphonique, car ceux-ci augmentent de manière exponentielle, en partie à cause de l'IA générative. Des capacités supplémentaires sont également nécessaires pour soutenir le bien-être du personnel des lignes d'assistance téléphonique et des premiers intervenants, et pour financer des enquêtes proactives susceptibles de mettre fin à la production et à la consommation de CSAM.[79] La formation dispensée par la police cambodgienne sur la CSEA facilitée par la technologie illustre comment mettre en place des systèmes inclusifs et centrés sur l'enfant.[220] De même, l'Association canadienne des chefs de police a adopté un cadre pour une police tenant compte des traumatismes, articulé autour de six étapes, le **modèle** des six « **R** » : Realize (prendre conscience), Recognize (reconnaître), Rethink (repenser), Respond (réagir), Reduce (réduire), Review (réviser).[221] Lorsque les systèmes tiennent compte des traumatismes et sont adaptés aux enfants, ils réduisent les effets néfastes de la culpabilisation des victimes, qui décourage le signalement, aggrave les conséquences à long terme et affaiblit la détection et la réponse.

> « Dans mon pays en particulier, je n'ai jamais vu personne blâmer la personne qui commet des abus. On entend toujours : ' Pourquoi as-tu fait ça ? C'est ton téléphone, pourquoi as-tu laissé cela se produire ? »

Jeune fille de 14 ans, Éthiopie[60]

Coordination intersectorielle mondiale pour lutter contre l'extorsion sexuelle financière

Une coordination mondiale entre les différents secteurs, notamment les forces de l'ordre, les gouvernements, l'industrie et les prestataires de services, est essentielle pour une prévention efficace, en particulier dans les cas d'extorsion financière à caractère sexuel. ECPAT recommande de renforcer davantage les mesures intersectorielles en :[222]

- En obligeant les institutions financières à détecter et à signaler activement les transactions liées à l'exploitation sexuelle des enfants.
- Adaptant les outils de surveillance aux nouvelles tendances, notamment les portefeuilles numériques et les cryptomonnaies.
- Réformant les lois sur le secret bancaire afin de permettre la collaboration avec les services de police au-delà de la police financière.

Prévenir l'extorsion sexuelle des enfants en ligne : aperçu du Centre australien de lutte contre l'exploitation des enfants, dirigé par la police fédérale australienne

Les données publiées par le Centre australien de lutte contre l'exploitation des enfants (ACCCE) en 2023 ont mis en évidence une nouvelle tendance : les délinquants étrangers ciblent principalement les adolescents de sexe masculin pour les extorquer financièrement à des fins sexuelles.[223] Plus de 90 % des signalements liés à l'extorsion financière à des fins sexuelles concernaient de jeunes victimes de sexe masculin. Les signalements d'extorsion sexuelle financière en ligne visant des enfants australiens ont augmenté de près de 60 % entre décembre 2022 et le début de l'année scolaire 2023, ce qui suggère une recrudescence pendant les vacances scolaires.[223]

Depuis janvier 2024, l'ACCCE a enregistré une baisse des signalements d'extorsion sexuelle financière, probablement grâce à la coordination des activités des forces de l'ordre, aux messages de prévention et aux efforts éducatifs. Cependant, de nombreux incidents ne seraient pas signalés, et l'extorsion sexuelle des enfants reste une préoccupation majeure et une priorité.

L'approche de l'ACCCE repose essentiellement sur une collaboration intersectorielle visant à diffuser des messages de prévention à grande échelle.

> « Pour que la prévention soit efficace, il faut tout un réseau et tout un écosystème. »

Forces de l'ordre[79]

Les partenariats réunissent les forces de l'ordre, l'industrie, les ONG et les organisations communautaires afin de toucher divers publics grâce à des interventions sur mesure. Voici quelques exemples :

- Sensibilisation ciblée des jeunes : l'ACCCE a collaboré avec Kids Helpline, Meta et le programme américain **NoFiltr** de prévention auprès des jeunes pour publier des ressources éducatives destinées aux 13-17 ans, fournissant des informations sur la manière de prévenir et de réagir à l'extorsion sexuelle. Ces ressources guident également les parents et les tuteurs sur la manière de reconnaître les risques, de signaler les incidents et d'accéder à une aide.[223]
- Prévention axée sur la famille : l'ACCCE a collaboré avec Project Paradigm à la campagne **« It's Never Too Early » (Il n'est jamais trop tôt)**, qui encourage les parents, les tuteurs et les futures familles à entamer très tôt des conversations sur la prévention des abus sexuels sur les enfants.[224]
- Campagnes de communication de masse : Afin d'atteindre directement les groupes à haut risque, l'ACCCE a développé une publicité animée de 30 secondes destinée aux garçons âgés de 13 à 17 ans, diffusée sur Snapchat, qui a touché environ cinq millions de personnes.[79, 225]

Figure 9. Campagne animée contre l'extorsion sexuelle sur Snapchat

- Éducation et formation : **ThinkUKnow**, dirigé par la police fédérale australienne, fournit aux écoles, aux familles et aux groupes communautaires des outils pratiques pour lutter contre les risques liés à la sécurité en ligne et à l'extorsion sexuelle. Les ressources comprennent des présentations, des fiches d'information, des cartes de conversation, des kits d'activités et du matériel adapté à la culture des communautés linguistiquement diverses, offrant ainsi de multiples points d'entrée pour discuter des risques en ligne.[152]

Bien que l'ACCCE collecte activement des données sur la participation, telles que le nombre de présentations données et le public atteint, il reste difficile de mesurer l'impact réel des efforts de prévention, car de nombreux résultats ne sont pas directement visibles dans les données. L'approche de l'ACCCE consiste à fournir aux parents et aux personnes qui s'occupent d'enfants des outils pratiques et des informations, en reconnaissant leur rôle clé dans la sécurité en ligne des enfants. Les efforts continus visent à atteindre les familles moins susceptibles de s'engager et à renforcer les initiatives d'éducation et de sensibilisation dans toutes les communautés.

Conclusion

La CSEA facilitée par la technologie est une menace mondiale qui peut être évitée. La tâche à accomplir est claire : combler les lacunes en matière de données probantes, identifier et développer les mesures efficaces, et accélérer la mise en œuvre des connaissances acquises. Dans un contexte de financement limité, cela signifie maximiser l'impact grâce au partage des connaissances et des données, à la coordination des programmes et aux enseignements tirés de la CSEA hors ligne et des efforts plus larges de prévention de la violence. Pour construire un monde numérique plus sûr, nous devons renforcer les maillons les plus faibles, en reconnaissant que les risques et les dangers migrent vers les espaces les moins protégés, et veiller à ce que chaque enfant bénéficie du même niveau de protection. Une prévention efficace passe par la mise en avant des droits et de la voix des enfants, par l'investissement dans des actions durables et fondées sur des données probantes, et par le renforcement de la collaboration entre tous les secteurs et toutes les parties prenantes. Grâce à une responsabilité partagée, la communauté internationale peut accélérer les progrès vers un environnement numérique plus sûr où les enfants peuvent apprendre, jouer et communiquer sans être victimes d'exploitation ou d'abus.

> « De la douleur à la détermination, de la survie à la force. »
>
> *Survivante, Philippines*[138]

Remerciements

Citation suggérée : WeProtect Global Alliance (2025). Global Threat Assessment 2025, Preventing technology-facilitated child sexual exploitation and abuse: From insights to action (by Lau LS, Mayevskaya Y, Fanton d'Andon C, Ware M, and Hermosilla S). WeProtect Global Alliance: https://www.weprotect.org/global-threat-assessment-25/

Auteurs

WeProtect Global Alliance

WeProtect Global Alliance est un mouvement mondial qui rassemble plus de 350 organisations gouvernementales, privées et civiles œuvrant pour transformer la réponse mondiale à l'exploitation et aux abus sexuels d'enfants en ligne.

Care and Protection of Children (CPC) Learning Network, Université Columbia

Le réseau d'apprentissage CPC, basé à la Mailman School of Public Health de l'université Columbia, promeut la santé et le bien-être des enfants par la recherche, les politiques et la pratique. Avec des partenaires dans plus de 20 pays, le CPC génère des données et des outils rigoureux et ancrés localement afin de renforcer les systèmes de protection de l'enfance et de promouvoir le bien-être des enfants, des jeunes et des familles à l'échelle mondiale.

Ce rapport a été rédigé par Ling San Lau, Yana Mayevskaya, Sabrina Hermosilla, Cécile Fanton d'Andon et Matthew Ware, avec la contribution supplémentaire de Claire Cunningham, Hannah Thompson, Cassie Landers, Hanna-Tina Fischer, Jonathan Huynh et Lisberma Peralta Aquino.

WeProtect Global Alliance tient à remercier toutes les organisations et toutes les personnes qui ont soutenu l'élaboration de l'Évaluation mondiale des menaces 2025. Nous exprimons notre profonde gratitude aux enfants et aux survivants dont les expériences et les témoignages ont nourri ce rapport et guident les efforts collectifs visant à assurer la sécurité des enfants. Le soutien apporté à l'élaboration du rapport, en tant que membre du comité directeur ou contributeur, n'implique pas l'approbation (partielle ou totale) du contenu de ce rapport.

Comité directeur d'experts

Aengus Ó Dochartaigh	MOORE | Prévention des abus sexuels sur les enfants, Université Johns Hopkins
Afrooz Kavani Johnson	UNICEF
Anil Raghuvanshi	ChildSafeNet
Beth Hepworth	PGI
Carolina Piñeros	RedPapaz
Dan Sexton	Fondation Internet Watch (IWF)
Debra Clelland	DeafKidz International
Elena Martellozzo	Childlight, Institut mondial pour la sécurité des enfants, Université d'Édimbourg
James Smith	PGI
Jess Lishak	Tech Coalition
Nina Vaaranen-Valkonen	Protéger les enfants
Ricardo de Lins e Horta	Gouvernement brésilien
Sambath Sokunthea	Gouvernement cambodgien
Soyoung Park	Autorité de régulation sud-coréenne, KCSC
Wirawan Boom Mosby	Projet HUG Thaïlande

Contributeurs

Les organisations suivantes ont fourni des informations provenant de survivants et de jeunes afin d'éclairer nos recherches :

VoiceBox

Une entreprise sociale britannique dirigée par des jeunes qui amplifie la voix des jeunes âgés de 13 à 25 ans. VoiceBox a organisé deux sessions avec des jeunes âgés de 14 à 18 ans provenant de sept pays, notamment des communautés marginalisées, des réfugiés et des survivants de génocide. Leurs points de vue ont nourri le rapport et le cadre de prévention.

Secrets Worth Sharing

Une organisation basée au Royaume-Uni qui encourage la discussion ouverte sur les abus sexuels pendant l'enfance par le biais de podcasts, d'ateliers et d'événements. Secrets Worth Sharing a examiné les outils de recherche qualitative et a apporté les points de vue des survivants qui ont été intégrés dans le rapport.

Fondation Marie Collins

Soutient les victimes et/ou les survivants d'abus sexuels sur mineurs assistés par la technologie, ainsi que leurs familles et les professionnels qui travaillent avec eux, en leur fournissant des services de défense, d'éducation et de rétablissement. La Fondation Marie Collins a examiné les outils de recherche qualitative, a apporté les points de vue des survivants et a animé un atelier avec des survivants afin d'examiner le cadre de prévention.

International Justice Mission (IJM) Philippines

Organisation mondiale qui lutte contre la traite des êtres humains, l'esclavage moderne, l'exploitation et les abus envers les enfants. L'IJM a apporté les points de vue des survivants pertinents pour le cadre de prévention et les a intégrés dans l'ensemble du rapport.

Footprints to Freedom

Une organisation basée aux Pays-Bas et dirigée par des survivants qui aide les victimes de la traite des êtres humains, met en œuvre des interventions locales en Ouganda, au Kenya et au Rwanda, et étend ses initiatives à travers l'Afrique grâce à sa Coalition africaine des survivants. Footprints to Freedom a apporté le point de vue des survivants dans l'ensemble du rapport.

Protect Children

Basée à Helsinki, Protect Children défend le droit de chaque enfant à être protégé contre les violences sexuelles, élabore des programmes de prévention, mène des recherches et aide à la réinsertion des délinquants. Protect Children a contribué à la rédaction de l'avant-propos rédigé par un survivant et a apporté des informations supplémentaires qui ont été intégrées dans l'ensemble du rapport.

Outre notre comité directeur d'experts, les personnes et organisations suivantes ont apporté leur expertise pour guider cette recherche :

- ECPAT
- Union européenne
- Réseau mondial des régulateurs de la sécurité en ligne (GOSRN)
- Google
- INHOPE
- Organisation internationale de police criminelle (INTERPOL)
- Fondation Lucy Faithfull
- Centre national pour les enfants disparus et exploités (NCMEC)
- Agence nationale contre la criminalité (NCA)
- Organisation nationale pour le traitement des abus (NOTA)
- Safe Futures Hub
- Snap
- Groupe de travail mondial virtuel (VGT)
- Forum économique mondial

Safe Futures Hub

Le cadre de prévention a été élaboré dans le cadre du Safe Futures Hub, une initiative conjointe de la Sexual Violence Research Initiative (SVRI), de Together for Girls et de la WeProtect Global Alliance, axée sur des solutions visant à mettre fin à la violence sexuelle contre les enfants.

La conception visuelle et la mise en page du rapport ont été réalisées par Rec Design. Le cadre de prévention a été conçu visuellement par Together Creative.

Se tenir au courant des nouvelles publications

Tableau 3. Sélection de publications en attente et de ressources evolutives

Nom de l'initiative	Description	Prévu
Disrupting Harm 2 (recherche menée conjointement par UNICEF Innocenti, ECPAT et INTERPOL)	Extension des enquêtes démographiques auprès des enfants et des personnes qui s'occupent d'eux, ainsi que des entretiens approfondis tenant compte des traumatismes subis par les jeunes survivants dans 12 pays supplémentaires, afin d'améliorer la compréhension mondiale de l'exploitation et des abus sexuels des enfants en ligne.	**2025-2026**
Global Boys Initiative (ECPAT)	Une publication à venir présentera une étude de cas au Pakistan avec des témoignages de survivants et de praticiens, mettant en évidence les initiatives visant à prévenir et à lutter contre l'exploitation sexuelle des garçons.	**2025-2026**
INSPIRE : Sept stratégies pour mettre fin à la violence à l'encontre des enfants (élaborées par l'OMS avec des partenaires mondiaux)	**INSPIRE** est un ensemble de mesures techniques classifiées en 7 stratégies et fondées sur des recherches scientifiques visant à prévenir la violence à l'égard des enfants âgés de 0 à 17 ans. Il aide les pays à coordonner des actions multisectorielles et à suivre les progrès accomplis.	**En cours**
Prévention mondiale (Prevention Global dans sa version anglaise) (mis en œuvre par MOORE | Prévention des abus sexuels sur les enfants, École de santé publique Johns Hopkins Bloomberg et Institut royal de recherche en santé mentale)	Lancé en 2024, **Prevention Global** est une plateforme de connaissances et une initiative de recherche ambitieuse qui évalue sept programmes développés pour prévenir les abus sexuels sur les enfants et mène des enquêtes de référence sur la prévalence de ces abus sur quatre continents (Brésil, Allemagne, Tanzanie et États-Unis).[176] Elle publie également des produits de connaissance explorant les aspects clés de la prévention, notamment **Serving Youth**, qui couvre la prévalence de la victimisation dans les environnements destinés aux jeunes aux États-Unis et fournit un guide pratique à l'intention des dirigeants ; **Scalability**, qui explore les obstacles et les possibilités d'extension des programmes ; et **Making The Case**, qui révèle la perception du public selon laquelle les abus sexuels sur les enfants sont un problème évitable.[125,176,226]	**2026**

Nom de l'initiative	Description	Prévu
Comportement responsable avec les jeunes et les enfants (RBYC)[74]	Le **RBYC** est un programme destiné aux 11-14 ans qui vise à prévenir les comportements sexuels problématiques et à aider les jeunes adolescents à développer des interactions sûres et appropriées – avec des enfants plus jeunes, leurs pairs et des adultes – tant en ligne que hors ligne. Il a été testé aux États-Unis et est actuellement adapté et évalué dans 24 écoles en Allemagne (22 dans le cadre d'essais contrôlés randomisés et 2 dans le cadre d'études pilotes).	**2026**
Safe Futures Hub Global Living Systematic Review and PbK Framework	Safe Futures Hub, en collaboration avec l'université d'Oxford, élabore actuellement une **revue systématique mondiale** afin de fournir des données continuellement mises à jour sur la prévention de la violence sexuelle envers les enfants, en mettant l'accent sur les pays à revenu faible et intermédiaire. En décembre 2025, le Hub lancera également son **cadre de connaissances fondées sur la pratique (PbK)**, qui reconnaît l'expertise acquise sur le terrain, fait entendre les voix sous-représentées et met en évidence pourquoi et comment les interventions réussissent dans des contextes réels.	**2025-2026**

Glossaire

Matériel d'abus sexuels d'enfants généré par l'intelligence artificielle (IA)	Utilisation abusive des technologies d'IA pour créer, en tout ou en partie, toute représentation sexualisée ou sexuellement explicite d'un enfant. Cela inclut les images, les vidéos, les fichiers audios, les animations ou tout autre média produit par l'IA. Il s'agit d'une forme de CSAM généré numériquement (DG-CSAM) (voir le terme associé « deepfakes »).[26]
Regroupement	Fonctionnalité qui regroupe les signalements liés à des incidents répandus, tels que des contenus viraux, en un seul signalement ou en un ensemble de signalements plus restreint, ce qui réduit les soumissions redondantes tout en conservant les informations sur tous les utilisateurs et incidents signalés.[12]
Chatbots	Outil conversationnel automatisé, souvent alimenté par l'IA, capable de simuler des enfants ou des adultes et d'interagir avec les utilisateurs en tant que compagnons, conseillers ou amis, mais pouvant présenter des risques tels que la désinformation, la collecte de données ou l'exposition à des contenus inappropriés.[59]
Matériel d'abus sexuels d'enfants (CSAM)	Matériel, tel que des images ou des vidéos, qui représente et/ou documente des actes d'abus sexuels et/ou d'exploitation d'enfants. Ce matériel peut être utilisé dans le cadre d'enquêtes criminelles et/ou servir de preuve dans des affaires pénales.[26]
Abus sexuels sur des enfants en ligne	Toute forme d'abus sexuel sur des enfants ayant un lien avec l'environnement numérique. Cela inclut les abus sexuels sur des enfants facilités par la technologie et ceux commis ailleurs, puis répétés en les partageant en ligne via les réseaux sociaux ou d'autres dimensions numériques.[26]
Exploitation sexuelle des enfants en ligne	Tous les actes de nature sexuelle commis à l'encontre d'un enfant et ayant un lien avec l'environnement numérique. Cela inclut toute utilisation de la technologie qui entraîne l'exploitation sexuelle ou conduit à l'exploitation sexuelle d'un enfant, ou qui entraîne ou conduit à la production, l'achat, la vente, la possession, la distribution ou la transmission d'images ou d'autres documents illustrant cette exploitation sexuelle. Par rapport aux abus, l'échange ou la distribution de contenu de valeur, y compris, mais sans s'y limiter, des images ou des vidéos, sont souvent des éléments constitutifs de l'exploitation.[26]
Deepfake	Un deepfake est un contenu généré par l'IA (par exemple, une photo, une vidéo, une animation ou un fichier audio) qui représente de manière réaliste une personne faisant ou disant quelque chose qu'elle n'a jamais fait.[227] Ce terme peut être utilisé pour désigner un contenu représentant de vrais enfants dans des situations sexuelles simulées.

Bien-être numérique	Impact des technologies sur la santé mentale, physique, sociale et émotionnelle d'un individu.[228]
Chiffrement de bout en bout	Méthode de sécurité qui garantit que seuls l'expéditeur et le destinataire prévu peuvent accéder au contenu d'une communication, empêchant ainsi les tiers, y compris les fournisseurs de services, de consulter ou de scanner les données.[229]
Intelligence artificielle générative (IA)	L'IA générative est une forme d'intelligence artificielle qui utilise des modèles d'apprentissage automatique pour analyser les modèles et la structure de ses données d'entraînement afin de créer de nouveaux contenus, notamment du texte, des images, des fichiers audio ou d'autres médias, qui imitent ces entrées.[230]
Grooming	Le grooming ou grooming en ligne désigne le processus consistant à établir/construire une relation avec un enfant, soit en personne, soit par le biais d'Internet ou d'autres technologies numériques, afin de faciliter les contacts sexuels avec cette personne. Dans le rapport, le terme « grooming » sans autre précision désigne le grooming à des fins sexuelles.[26]
Comportements sexuels préjudiciables	Actions sexuelles initiées par un enfant ou une jeune personne qui sont inappropriées sur le plan du développement, coercitives ou abusives, et qui peuvent causer du tort à eux-mêmes ou à autrui. Les comportements sexuels problématiques désignent les actions sexuelles qui peuvent être inappropriées ou préoccupantes, mais qui ne répondent pas aux critères de préjudice ou d'abus. Le présent rapport utilise le terme « comportements sexuels préjudiciables » pour englober tout l'éventail des comportements préoccupants, tout en reconnaissant que les comportements à un stade précoce ou moins graves nécessitent néanmoins une intervention afin d'éviter qu'ils ne s'aggravent.[108]
Correspondance de hachage	Un algorithme appelé « fonction de hachage » est utilisé pour calculer une empreinte digitale, appelée « hachage », à partir d'un fichier. La comparaison d'un tel hachage avec un autre hachage stocké dans une base de données est appelée « correspondance de hachage ». Dans le contexte de la sécurité en ligne, la correspondance de hachage peut être un moyen essentiel pour détecter et prévenir la circulation des images et des vidéos illégales ou autrement préjudiciables déjà connues.[231]
Abus diffusés en direct (Livestreamed)	Souvent transmis aux spectateurs via des plateformes de diffusion en direct dédiées ou les réseaux sociaux, le contenu est diffusé instantanément, ce qui permet aux spectateurs de regarder et de participer pendant que l'abus est en cours. Par rapport à d'autres formats, cela peut laisser moins de traces numériques de l'abus.[26]
Partage non consensuel d'images intimes (NCII)	Terme couramment associé aux adultes qui désigne le partage d'images à caractère sexuel ou sexuellement suggestif sans le consentement de la personne représentée. Cela peut se produire lorsque des contenus initialement partagés de manière consensuelle sont ensuite partagés ou transmis sans consentement, ou lorsque des photos sont prises sans consentement (par exemple dans le cadre de grooming ou d'extorsion sexuelle). Le concept clé est la « perte de contrôle » sur les représentations.[26] Ce terme doit être utilisé avec prudence lorsqu'il est appliqué à des enfants qui n'ont pas atteint l'âge du consentement sexuel (voir le contenu sexuel autoproduit impliquant des enfants).

Délinquant	Personne qui a commis des infractions ou qui est coupable d'un crime impliquant l'exploitation et l'abus sexuels d'enfants.[26]
Séduction en ligne	Lorsqu'une personne communique avec un enfant via Internet (ou une autre technologie) dans l'intention de commettre une infraction sexuelle ou un enlèvement.[232]
Auteur	Personne qui peut avoir participé à l'exploitation sexuelle d'enfants (indépendamment de son implication dans le processus pénal). Nous utilisons les termes « auteur » et « auteur potentiel » pour désigner les personnes qui ont commis ou pourraient commettre ces actes, qu'elles répondent ou non à la définition spécifique d'un crime ou qu'elles aient été arrêtées/condamnées pour un crime.[26]
Contenu à caractère sexuel impliquant des enfants, autoproduit	Les enfants et les adolescents de moins de 18 ans peuvent prendre des photos ou enregistrer des vidéos à caractère sexuel d'eux-mêmes. Bien que ce comportement ne soit pas nécessairement illégal ou socialement inacceptable en soi, il existe un risque que ce type de contenu soit diffusé en ligne ou en personne dans le but de nuire aux enfants ou d'être utilisé à des fins d'extorsion. Nous utilisons ce terme, ainsi que celui de « sexting », qui est une référence courante dans le langage familier pour désigner le fait de prendre et de partager des images à caractère sexuel. Les enfants disent souvent qu'ils ne comprennent pas la notion de contenu « auto-généré » et, dans des contextes tels que le partage non consensuel, cela peut être inutile.[233]
Extorsion sexuelle des enfants	Processus par lequel les enfants sont contraints de continuer à produire du matériel à caractère sexuel et/ou à accomplir des actes pénibles sous la menace de divulguer à d'autres le matériel les représentant. Lorsque la motivation est principalement financière, nous utilisons également le terme « extorsion sexuelle financière ».[26]
Survivant	Personnes qui ont subi des préjudices et des victimisations. L'utilisation du terme « survivant » peut refléter un processus de guérison. Reconnaissant la diversité des préférences terminologiques des personnes ayant vécu cette expérience, nous utilisons les termes « victime » et « survivant » de manière interchangeable dans le rapport.[26]
Exploitation et abus sexuels d'enfants facilités par la technologie (CSEA facilitée par la technologie, également appelés TFCSEA)	L'exploitation et les abus sexuels envers les enfants facilités par la technologie désignent l'utilisation des technologies numériques à n'importe quelle étape pour préparer, commettre ou diffuser (dans le cas du CSAM) l'exploitation ou les abus sexuels d'un enfant. Cela englobe les préjudices commis dans des environnements numériques et non numériques (hors ligne), y compris, par exemple, l'échange d'informations, la coordination d'actions et la prise de contact avec des enfants dans le but de les manipuler ou de les contraindre. Ce terme reconnaît que les technologies jouent un rôle dans la facilitation des abus et la perpétuation des préjudices causés par ces abus, tant dans les espaces physiques que numériques.[26]
Victime	Personnes qui ont été victimes d'actes préjudiciables et/ou criminels en tant que titulaires de droits. Reconnaissant la diversité des préférences terminologiques des personnes ayant vécu cette expérience, nous utilisons ce terme de manière interchangeable avec « survivant » dans le rapport.[26]

Références

1. Navigating the Unknown: Reflections on AI, the Metaverse, and Keeping Young People Safe | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/navigating-unknown-reflections-ai-metaverse-and-keeping-young-people-safe
2. MOORE | Preventing Child Sexual Abuse | Johns Hopkins Bloomberg School of Public Health [Internet]. [cited 2025 Sept 27]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse
3. United Nations Department of Economic and Social Affairs [Internet]. Global Internet Use Continues To Rise But Disparities Remain. [cited 2025 Nov 20]. Available from: https://social.desa.un.org/sdn/global-internet-use-continues-to-rise-but-disparities-remain
4. GSMA. Smartphone owners are now the global majority, New GSMA report reveals [Internet]. Newsroom. 2023 [cited 2025 Nov 4]. Available from: https://www.gsma.com/newsroom/press-release/smartphone-owners-are-now-the-global-majority-new-gsma-report-reveals/
5. ITU. Statistics [Internet]. [cited 2025 Nov 21] . Available from: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx
6. Generative AI: Risks and opportunities for children | Innocenti Global Office of Research and Foresight [Internet]. [cited 2025 Aug 29]. Available from: https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children
7. Industry. Data collected by the CPC Learning Network through key informant interviews.
8. Academic. Data collected by the CPC Learning Network through key informant interviews.
9. Intergovernmental. Data collected by the CPC Learning Network through key informant interviews.
10. Safe Online. Disrupting Harm [Internet]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf
11. Civil Society. Data collected by the CPC Learning Network through key informant interviews.
12. National Center for Missing and Exploited Children. CyberTipline Data [Internet]. [cited 2025 Sept 3]. Available from: https://ncmec.org/gethelpnow/cybertipline/cybertiplinedata
13. INHOPE Releases Annual Report 2024 [Internet]. [cited 2025 May 5]. Available from: https://inhope.org/EN/articles/inhope-annual-report-2024
14. IWF 2024 Annual Data & Insights Report [Internet]. [cited 2025 May 6]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/
15. How AI is being abused to create child sexual abuse material (CSAM) online [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

16. 118th Congress. S.474 - REPORT Act [Internet]. 2024. Available from: https://www.congress.gov/bill/118th-congress/senate-bill/474

17. UK Public General Acts. Online Safety Act 2023 [Internet]. 50 Oct 26, 2023. Available from: https://www.legislation.gov.uk/ukpga/2023/50

18. Social media ban in Australia | A simple guide [Internet]. UNICEF Australia. [cited 2025 Sept 27]. Available from: https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer?srsltid=AfmBOop6gJckegYUrtle7BkiDMa6ZKUVy0aaGjHrYShDthWRHUqp8_9A

19. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.211, DE 17 DE SETEMBRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

20. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.100, DE 13 DE JANEIRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15100.htm

21. New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users [Internet]. Infocomm Media Development Authority. [cited 2025 Aug 29]. Available from: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services

22. Making the digital and physical world safer: Why the Convention against Cybercrime matters | UN News [Internet]. 2024 [cited 2025 Sept 27]. Available from: https://news.un.org/en/story/2024/12/1158526

23. UN Cybercrime Convention - Full Text [Internet]. United Nations : Office on Drugs and Crime. [cited 2025 Aug 25]. Available from: //www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

24. Global Digital Compact | Office for Digital and Emerging Technologies [Internet]. [cited 2025 Sept 10]. Available from: https://www.un.org/digital-emerging-technologies/global-digital-compact

25. Lantern: advancing child safety through signal sharing [Internet]. https://technologycoalition.org/. [cited 2025 Sept 27]. Available from: https://technologycoalition.org/programs/lantern/

26. ECPAT. Terminology Guidelines [Internet]. 2025 [cited 2025 Aug 29]. Available from: https://ecpat.org/terminology/

27. Call for consultants, global Living Systematic Review consultant(s):... [Internet]. Safe Futures Hub. [cited 2025 Sept 27]. Available from: https://www.safefutureshub.org/call-for-consultants-global-living-systematic-review-consultants-what-works-to-prevent-childhood-sexual-violence

28. Prevention Global. Prevention Global launches with new online resource hub and landmark impact evaluations [Internet]. [cited 2025 Sept 27]. Available from: https://www.prevention.global/

29. Model National Response to end child sexual exploitation & abuse online - WeProtect Global Alliance [Internet]. 2020 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/frameworks/model-national-response/

30. Bronfenbrenner U. Toward an experimental ecology of human development. Am Psychol. 1977;32(7):513–31.

31. UNICEF. Corporate reporting on child rights in relation to the digital environment [Internet]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/reporting

32. Workshop. Data collected by the CPC Learning Network through key informant interviews.

33. Convention on the Rights of the Child, 20 November 1989 [Internet]. [cited 2025 Sept 10]. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/crc-1989

34. OHCHR. General comment No. 25 (2021) on children's rights in relation to the digital environment [Internet]. OHCHR. [cited 2025 Nov 3]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

35. United Nations. Guiding Principles on Business and Human Rights : Implementing the United Nations "Protect, Respect and Remedy" Framework [Internet]. Available from: https://digitallibrary.un.org/record/720245?v=pdf

36. UNICEF. Children's Rights Business Principles 2012 [Internet]. [cited 2025 Nov 3]. Available from: https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf

37. WeProtect Global Alliance. Children and Young People present their roadmap for a safer digital world [Internet]. Available from: https://www.weprotect.org/news/children-and-young-people-present-their-roadmap-for-a-safer-digital-world/

38. SafetyNet: insights from young people around the world [Internet]. Safe Futures Hub. [cited 2025 Sept 22]. Available from: https://www.safefutureshub.org/resources/safetynet-insights-from-young-people-around-the-world

39. Thorn. Evolving Technologies Horizon Scan [Internet]. Available from: https://www.thorn.org/research/library/evolving-technologies-horizon-scan/

40. UNICEF. Childhood in a Digital World [Internet]. [cited 2025 Nov 20]. Available from: https://www.unicef.org/innocenti/reports/childhood-digital-world

41. 10 countries with the highest percentage of web traffic from mobile phones | Business Insider Africa [Internet]. [cited 2025 Aug 29]. Available from: https://africa.businessinsider.com/local/lifestyle/10-countries-with-the-highest-percentage-of-web-traffic-from-mobile-phones/04wvy3f

42. Facts and Figures 2024 - Youth Internet use [Internet]. [cited 2025 Aug 29]. Available from: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-youth-internet-use

43. Slater SO, Arundell L, Grøntved A, Salmon J. Age of first digital device use and screen media use at age 15: A cross-sectional analysis of 384,591 participants from 55 countries. Public Health Pract [Internet]. 2025 June 1 [cited 2025 Sept 2];9:100596. Available from: https://www.sciencedirect.com/science/article/pii/S2666535225000151

44. Coded Companions: Young People's Relationships With AI Chatbots | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/coded-companions-young-peoples-relationships-ai-chatbots

45. Snap Digital Well-Being Index | Snapchat Safety [Internet]. [cited 2025 Sept 27]. Available from: https://values.snap.com/safety/dwbi

46. Häubi RB. How the UN plans to connect every school to the internet by 2030 [Internet]. SWI swissinfo.ch. 2024 [cited 2025 Sept 2]. Available from: https://www.swissinfo.ch/eng/international-geneva/the-un-plans-to-connect-every-school-to-the-internet-by-2030/83325727

47. Peng D, Yu Z. A Literature Review of Digital Literacy over Two Decades. Educ Res Int [Internet]. 2022 [cited 2025 Sept 3];2022(1):2533413. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/2533413

48. World Health Organization. 1st Global Ministerial Conference on Ending Violence Against Children [Internet]. [cited 2025 Nov 4]. Available from: https://www.who.int/teams/social-determinants-of-health/violence-prevention/1st-global-ministerial-conference-on-ending-violence-against-children

49. INHOPE. Launching Version 3 of the Universal Classification Schema [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://inhope.org/EN/articles/what-s-new-in-version-3-of-the-universal-classification-schema

50. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update January 2025.

51. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update June 2025.

52. Patchin JW, Hinduja S. The nature and extent of youth sextortion: Legal implications and directions for future research. Behav Sci Law. 2024;42(4):401–16.

53. MikeHarrison. Global Taskforce on child sexual abuse online - WeProtect Global Alliance [Internet]. 2022 [cited 2025 Nov 3]. Available from: https://www.weprotect.org/global-taskforce-on-child-sexual-abuse-online/

54. Government. Data collected by the CPC Learning Network through key informant interviews.

55. Transparency reporting on child sexual exploitation and abuse online [Internet]. 2023 Sept [cited 2025 Sept 30]. (OECD Digital Economy Papers; vol. 357). Report No.: 357. Available from: https://www.oecd.org/en/publications/transparency-reporting-on-child-sexual-exploitation-and-abuse-online_554ad91f-en.html

56. Grossman S, Pfefferkorn R, Thiel D, Shah S, DiResta R, Perrino J, et al. The Strengths and Weaknesses of the Online Child Safety Ecosystem. 2024 Apr 22 [cited 2025 Sept 5]; Available from: https://purl.stanford.edu/pr592kc5483

57. Childlight Into the Light Index [Internet]. [cited 2025 Apr 30]. Available from: https://www.childlight.org/into-the-light

58. 2024 Annual Report [Internet]. National Center for Missing & Exploited Children. [cited 2025 Aug 25]. Available from: http://www.missingkids.org/content/ncmec/en/footer/about/annual-report.html

59. UNICEF. The risky new world of tech's friendliest bots [Internet]. Available from: https://www.unicef.org/innocenti/stories/risky-new-world-techs-friendliest-bots

60. Data from the youth consultations led by Voicebox.

61. Davis P. Spike in online crimes against children a "wake-up call" [Internet]. National Center for Missing & Exploited Children. [cited 2025 Sept 27]. Available from: http://www.ncmec.org/content/ncmec/en/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call.html

62. Deepfake Nudes & Young People: Navigating a New Frontier in Technology-facilitated Nonconsensual Sexual Abuse and Exploitation [Internet]. Thorn. [cited 2025 Sept 5]. Available from: https://www.thorn.org/research/library/deepfake-nudes-and-young-people/

63. Online child sex abuse material, boosted by AI, is outpacing Big Tech's regulation [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/iwf-in-the-news/online-child-sex-abuse-material-boosted-by-ai-is-outpacing-big-techs-regulation/

64. Thiel D, DiResta R, Stamos A. Cross-Platform Dynamics of Self-Generated CSAM. 2023 June 6 [cited 2025 Aug 25]; Available from: https://fsi.stanford.edu/publication/cross-platform-dynamics-self-generated-csam

65 How Instagram's Algorithm Connects and Promotes Pedophile Network - Tech News Briefing - WSJ Podcasts [Internet]. [cited 2025 Aug 25]. Available from: https://www.wsj.com/podcasts/tech-news-briefing/how-instagrams-algorithm-connects-and-promotes-pedophile-network/A683C0B4-2E6F-4661-9973-10BD455DB895

66. AI enabling 'DIY child abuse' tools, with child victims in models, IWF warns MPs [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/ai-giving-offenders-diy-child-sexual-abuse-tool-as-dozens-of-child-victims-used-in-ai-models-iwf-warns-mps/

67. Aws Ai, Hugging Face, Inflection, Metaphysic, Stability AI, Teleperformance. Safety by Design for Generative AI: Preventing Child Sexual Abuse. Thorn [Internet]. 2024; Available from: https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf

68. Thorn. Synthetic Media Framework Case Study: Thorn. [cited 2025 Nov 4]; Available from: https://partnershiponai.org/wp-content/uploads/2024/11/case-study-thorn.pdf

69. Sivathasan N, Clahane P, Kemoli D. TikTok profiting from sexual livestreams involving children, BBC told. BBC [Internet]. 2025 Mar 2; Available from: https://www.bbc.com/news/articles/cedl8eyy4pjo

70. Ovaska A, Insoll T, Soloveva V, Vaaranen-Valkonen N, Di GR. Findings from Italian language respondents to Re-Direction surveys of CSAM users on dark web search engine. JRC Publ Repos [Internet]. 2025 [cited 2025 Nov 3]; Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC138231

71. FATF Annual Report 2023-2024 [Internet]. [cited 2025 Sept 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html

72. Protect Children. Tech Platforms Used by Online Child Sexual Abuse Offenders [Internet]. 2024. Available from: https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

73. Ending the Scourge: The Need for the STOP CSAM Act — Testimony of Michelle DeLaune, President and CEO, National Center for Missing & Exploited Children (PDF) [Internet]. Room 226, Dirksen Senate Office Building, Washington, DC; 2025 [cited 2025 Sept 5]. p. 16. Available from: https://www.judiciary.senate.gov/imo/media/doc/2025-03-11_testimony_delaune.pdf

74. Responsible Behavior with Youth and Children | MOORE | Preventing Child Sexual Abuse [Internet]. [cited 2025 Sept 5]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse/responsible-behavior-with-youth-and-children

75. The emergence of immersive technologies and Extended Reality - WeProtect Global Alliance [Internet]. [cited 2025 May 1]. Available from: https://www.weprotect.org/thematic/extended-reality/

76. Child safeguarding and immersive technologies [Internet]. NSPCC Learning. [cited 2025 Aug 25]. Available from: https://learning.nspcc.org.uk/research-resources/2023/child-safeguarding-immersive-technologies

77. Data from Marie Collins Foundation survivor consultation session.

78. Edwards G, Christensen L. Cyber strategies used to combat child sexual abuse material [Internet]. Australian Institute of Criminology; 2021 [cited 2025 Nov 4]. Available from: https://www.aic.gov.au/publications/tandi/tandi636

79. Law enforcement. Data collected by the CPC Learning Network through key informant interviews.

80. Walsh K, Mathews B, Parvin K, Smith R, Burton M, Nicholas M, et al. Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. Child Abuse Negl. 2025 Feb;160:N.PAG-N.PAG.

81. Under 10s groomed online 'like never before' in 2023 find IWF [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/under-10s-groomed-online-like-never-before-as-hotline-discovers-record-amount-of-child-sexual-abuse/

82. Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/girls-young-women-led-assessment-on-online-sexual-exploitation-abuse-technology-facilitated-gender-based-violence-in-africa/

83. Protecting Children From Violence and Exploitation in Relation to the Digital Environment | UNICEF [Internet]. [cited 2025 Sept 5]. Available from: https://www.unicef.org/documents/protecting-children-violence-and-exploitation-relation-digital-environment

84. Huang TF, Chun-Yin H, Fong-Ching C, Fong-Ching C, Chiu CH, Ping-Hung C, et al. Adolescent Use of Dating Applications and the Associations with Online Victimization and Psychological Distress. Behav Sci [Internet]. 2023;13(11):903. Available from: https://pubmed.ncbi.nlm.nih.gov/37998650/

85. Technology-facilitated Child Sexual Exploitation and Sexual Abuse in Burkina Faso, Côte d'Ivoire, Guinea and Niger [Internet]. ECPAT. [cited 2025 Sept 5]. Available from: https://ecpat.org/resource/technology-facilitated-child-sexual-exploitation-and-sexual-abuse-in-burkina-faso-cote-divoire-guinea-and-niger/

86. Pinto Cortez, Cristián & Guerra, Cristobal. Parental styles and online sexual abuse prevention factors. 2024. Límite (Arica). 19. 1-9. 10.4067/s0718-50652024000100209. Available from: https://www.researchgate.net/publication/383135600_Parental_styles_and_ online_sexual_abuse_prevention_factors

87. Wright MF. The Associations among Cyberbullying Victimization and Chinese and American Adolescents' Mental Health Issues: The Protective Role of Perceived Parental and Friend Support. Int J Environ Res Public Health [Internet]. 2024;21(8). Available from: https://pubmed.ncbi.nlm.nih.gov/39200678/

88. Friedman-Hauser G, Katz C. "She has a history of making things up": Examining the disclosure and reporting of online sexual abuse among children with disabilities. Child Abuse Negl [Internet]. 2025;163 ((Friedman-Hauser G., galf@haruv.org.il) The Bob Shapell School of Social Work, Tel Aviv University, Israel). Available from: https://awspntest.apa.org/record/2026-05574-001

89. Wright MF, Wachs S. Longitudinal
Associations between Different Types of Sexting, Adolescent Mental Health, and Sexual Risk Behaviors: Moderating Effects of Gender, Ethnicity, Disability Status, and Sexual
Minority Status. Arch Sex Behav [Internet]. 2024 Mar 1 [cited 2025 Sept 30];53(3):1115–28. Available from: https://doi.org/10.1007/s10508-023-02764-7

90. Gemara N, Mishna F, Katz C. 'If my parents find out, I will not see my phone anymore': Who do children choose to disclose online sexual solicitation to? Child Fam Soc Work [Internet]. 2025 [cited 2025 Sept 5];30(1):4–14. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/cfs.13069

91. Lusky-Weisrose E, Klebanov B, Friedman-Hauser G, Avitan I, Katz C. Online sexual abuse of children with disabilities: Analyzing reports of social workers' case files in Israel. Child Abuse Negl. 2024 Aug;154:N. PAG-N.PAG.

92. Hong JS, Kim J, Lee JM, Saxon S, Thornberg R. Pathways from Polyvictimization to Offline and Online Sexual Harassment Victimization Among South Korean Adolescents. Arch Sex Behav. 2023 Oct;52(7):2779–88.

93. Tanaya NLTP, Puteri NMM. Child Sexual Abuse and Exploitation through Livestreaming in Indonesia: Unequal Power Relations at the Root of Child Victimization. J Int Womens Stud [Internet]. 2023 Apr;25(3):1–14. Available from: https://vc.bridgew.edu/jiws/vol25/iss3/6

94. Children P. What Drives Online Child Sexual Abuse Offending? Understanding Motivations, Facilitators, Situational Factors, and Barriers [Internet]. Protect Children. 2024 [cited 2025 Aug 31]. Available from: https://www.suojellaanlapsia.fi/en/post/2know-final-report-1

95. Napier SS, Seto MC, Cashmore J, Shackel R. Characteristics that predict exposure to and subsequent intentional viewing of child sexual abuse material among a community sample of Internet users. Child Abuse Negl. 2024 Oct;156:106977.

96. Lahtinen HM, Honkalampi K, Insoll T, Nurmi J, Quayle E, Ovaska AK, et al. Investigating the disparities among child sexual abuse material users: Anonymous self-reports from both charged and uncharged individuals. Child Abuse Negl. 2025 Mar;161:107299.

97. Chauviré-Geib K, Gerke J, Fegert JM, Rassenhofer M. The Digital Dimension: Victim's Experiences of Technology's Impact on Penetrative Child Sexual Abuse. J Child Sex Abuse. 2025 Apr 28;1–21.

98. Christensen LS, Woods J. "It's Like POOF and It's Gone": The Live-Streaming of Child Sexual Abuse. Sex Cult. 2024 Aug 1;28(4):1467–81.

99. Ringrose J, Regehr K. Recognizing and addressing how gender shapes young people's experiences of image-based sexual harassment and abuse in educational settings. J Soc Issues. 2023 Dec;79(4):1251–81.

100. 20 arrested in international operation targeting child sexual abuse material [Internet]. [cited 2025 Sept 30]. Available from: https://www.interpol.int/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material

101. 25 arrested in global hit against AI-generated child sexual abuse material [Internet]. Europol. [cited 2025 Sept 30]. Available from: https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

102. UNICEF. Who Perpetrates Online Child Sexual Exploitation and Abuse? [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf

103. Child sexual abuse material (CSAM) [Internet]. Thorn. [cited 2025 Sept 30]. Available from: https://www.thorn.org/research/child-sexual-abuse-material-csam/

104. Salter M, Wong T. Parental Production of Child Sexual Abuse Material: A Critical Review. Trauma Violence Abuse. 2024 July;25(3):1826–37.

105. Finkelhor D, Turner H, Colburn D. The prevalence of child sexual abuse with online sexual abuse added. Child Abuse Negl. 2024;149.

106. Finkelhor D, Shattuck A, Turner HA, Hamby SL. The lifetime prevalence of child sexual abuse and sexual assault assessed in late adolescence. J Adolesc Health. 2014;55(3):329-333.

107. Russell DH, Trew S, Smith R, Higgins DJ, Walsh K. Primary prevention of harmful sexual behaviors by children and young people: A systematic review and narrative synthesis. Aggress Violent Behav. 2025 Apr;81:N. PAG-N.PAG.

108. Safe Futures Hub. Children Displaying Harmful Sexual Behaviour: Evidence and Responses [Internet]. 2025 [cited 2025 Nov 4]. Available from: https://cdn.safefutureshub.org/files/Children-displaying-harmful-sexual-behaviour-Evidence-and-responses.pdf

109. Tunagur MT, Oksal H, Büber Ö, Kurt Tunagur EM, Sarıgedik E. Risk Factors and Predictors of Penetrative Online Child Sexual Abuse. J Pediatr Health Care. 2025;39(2):198–205.

110. Leaked: Understanding and Addressing Self-Generated Sexual Content involving Young People in Thailand [Internet]. Evident. [cited 2025 Sept 6]. Available from: https://www.itsevident.org/major-projects

111. Disrupting Harm country reports | Innocenti Global Office of Research and Foresight [Internet]. 2022 [cited 2025 Sept 6]. Available from: https://www.unicef.org/innocenti/reports/disrupting-harm-country-reports

112. Trends and insights from a unique helpline preventing child sexual abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 5]. Available from: https://www.lucyfaithfull.org.uk/research/trends-and-insights-from-a-unique-helpline-preventing-child-sexual-abuse/

113. Bailey A, Allen L, Stevens E, Dervley R, Findlater D, Wefers S. Pathways and Prevention for Indecent Images of Children Offending: A Qualitative Study. Sex Offending Theory Res Prev [Internet]. 2022 Dec 2 [cited 2025 Sept 5];17:1–24. Available from: https://sotrap.psychopen.eu/index.php/sotrap/article/view/6657

114. Protect Children. Our Voice Male Survivors: Experiences of Victims and Survivors of Child Sexual Abuse and Exploitation [Internet]. 2025. Available from: https://www.suojellaanlapsia.fi/en/post/our-voice-male-survivors

115. Tech Coalition | Assessing OCSEA Harms in Product Development [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/assessing-ocsea-harms-in-product-development

116. Detecting, Disrupting and Investigating Online Child Sexual Exploitation [Internet]. [cited 2025 Aug 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

117. Internet Watch Foundation. Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports [Internet]. 2024 [cited 2025 Nov 10]. Available from: https://www.iwf.org.uk/news-media/news/teenage-boys-targeted-as-hotline-sees-heartbreaking-increase-in-child-sextortion-reports/

118. Self-Generated Child Sexual Abuse Fieldwork Findings Report by PIER [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/self-generated-child-sexual-abuse-fieldwork-findings-report/

119. MikeHarrison. Link-sharing and child sexual abuse: understanding the threat - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/library/link-sharing-and-child-sexual-abuse-understanding-the-threat/

120. Iyer C, Mehra S. Not a Child's Play: Taking Stock of Children's Gaming in India, Gaps, Emerging Risks and Responses [Internet]. Space2Grow; 2025 June. Available from: https://www.space2grow.in/_files/ugd/fcdbc5_0dead6ef6615455280abdbded0c2c605.pdf

121. Situation Analysis of Child Online Protection in Pakistan | UNICEF Pakistan [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/pakistan/documents/situation-analysis-child-online-protection-pakistan

122. Online sexual abuse of primary children 1000% worse since lockdown [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/sexual-abuse-imagery-of-primary-school-children-1-000-per-cent-worse-since-lockdown/

123. CDC. A Public Health Approach to Community Violence Prevention [Internet]. Community Violence Prevention. 2025 [cited 2025 Sept 22]. Available from: https://www.cdc.gov/community-violence/php/public-health-strategy/index.html

124. Emery CR, Wong PWC, Haden-Pawlowski V, Pui C, Wong G, Kwok S, et al. Neglect, online invasive exploitation, and childhood sexual abuse in Hong Kong: Breaking the links. Child Abuse Negl. 2024 Jan;147:N.PAG-N.PAG.

125. Scalability | Prevention Global [Internet]. [cited 2025 Sept 22]. Available from: https://www.prevention.global/scalability

126. 2024: A Year of Urgency, Vision, and Partnership in Safeguarding Children Online – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/2024-a-year-of-urgency-vision-and-partnership-in-safeguarding-children-online/

127. Safe Online. Financing a Safe Digital Future: Safer Internet Day 2025 – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/financing-a-safe-digital-future-safer-internet-day-2025/

128. Ending Online Child Sexual Exploitation and Abuse | UNICEF [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/documents/ending-online-child-sexual-exploitation-and-abuse

129. Kardefelt-Winther D, Maternowska C. Addressing violence against children online and offline. Nat Hum Behav. 2020;4:227–30.

130. Data for Change – Safe Online [Internet]. [cited 2025 Sept 27]. Available from: https://safeonline.global/data-for-change/

131. UNICEF. Data brief on Measuring Technology-facilitated Violence against Children in line with the International Classification of Violence against Children (ICVAC) [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://data.unicef.org/resources/data-brief-on-measuring-technology-facilitated-violence-against-children-in-line-with-the-international-classification-of-violence-against-children-icvac/

132. Safe Future Hub [Internet]. Available from: https://www.safefutureshub.org

133. Sexual Violence Research Initiative. SVRI Building the Field [Internet]. Available from: https://www.svri.org

134. Together for Girls [Internet]. Available from: https://www.togetherforgirls.org/

135. WeProtect Global Alliance. A global commitment to every child [Internet]. Available from: https://www.weprotect.org

136. General comment No. 24 (2019) on children's rights in the child justice system | OHCHR [Internet]. [cited 2025 Sept 22]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2019-childrens-rights-child

137. Reason J. The contribution of latent human failures to the breakdown of complex systems. Philos Trans R Soc Lond B Biol Sci [Internet]. 1997 Jan [cited 2025 Sept 27];327(1241):475–84. Available from: https://royalsocietypublishing.org/doi/10.1098/rstb.1990.0090

138. Data from the Philippines Survivor Network consultations with survivors.

139. Lundy L. 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child. Br Educ Res J. 2007;33(6):927–42.

140. O'Kane C. Active and Safe: The Global Program Guide for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/efpp/Active_%26amp%3B_Safe_GUIDE/

141. O'Kane C. Active and Safe: Accompanying Toolkit for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/kqad/Active_%26_Safe_TOOLKIT_web_19Aug2025/

142. UNICEF. Spotlight guidance on best practices for stakeholder engagement with children in D-CRIAs [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.unicef.org/childrightsandbusiness/reports/D-CRIA-Spotlight-guidance-stakeholder-engagement

143. Diagram adapted from Lansdown G, Haj-Ahmead J, Rusinow T, Sukura Y Friscia. Conceptual Framework for Measuring Outcomes of Adolescent Participation [Internet]. 2018 [cited 2025 Nov 4]. Available from: https://www.unicef.org/media/59006/file

144. WeProtect Global Alliance. Visualising child and survivor participation [Internet]. Available from: https://www.weprotect.org/response/child-survivor-participation/mapping-participation-initiatives/#dataviz

145. European Union. BeSmartOnline - Maltese Safer Internet Centre [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://better-internet-for-kids.europa.eu/en/saferinternetday/malta

146. Be Smart Online. A Safer Internet for Malta [Internet]. [cited 2025 Oct 29]. Available from: https://www.besmartonline.info

147. VoiceBox. VoiceBox | By young people, for young people [Internet]. [cited 2025 Nov 4]. Available from: https://voicebox.site/

148. How can service providers work with boys at-risk and survivors of sexual exploitation and abuse in a gender-sensitive way? [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/story/global-boys-initiative-case-studies/

149. SecretsWorthSharing. Secrets Worth Sharing | How to talk about childhood sexual abuse [Internet]. SecretsWorthSharing. [cited 2025 Nov 4]. Available from: https://www.secretsworthsharing.com

150. CPC Learning Network. Secrets Worth Sharing founder testimony.

151. Global Threat Assessment 2023 Data - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/global-threat-assessment-23/data/

152. Resources | ThinkUKnow [Internet]. [cited 2025 Sept 22]. Available from: https://www.thinkuknow.org.au/resources-tab

153. World Vision. Tackling Online Child Sexual Exploitation [Internet]. [cited 2025 Oct 29]. Available from: https://wvi.org.vn/special-projects/tackling-online-child-sexual-exploitation-ene29.html

154. End Violence. More progress and impact from our grantees [Internet]. End Violence. [cited 2025 Nov 4]. Available from: https://www.end-violence.org/node/7971

155. UNICEF. Parenting for the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: www.unicef.org/documents/parenting-digital-age

156. National Crime Agency. National Crime Agency launches online campaign to tackle "sextortion" among young teenage boys [Internet]. Available from: https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-launches-online-campaign-to-tackle-sextortion-among-young-teenage-boys

157. Think Before You Share Campaign from IWF [Internet]. [cited 2025 Sept 17]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/think-before-you-share/

158. UNODC. Beware The Share [Internet]. [cited 2025 Nov 4]. Available from: www.unodc.org/roseap/uploads/documents/beware-the-share/index.html

159. Safe Online. Grantee Highlight – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/grantee-highlight/

160. Letourneau EJ, Schaeffer CM, Bradshaw CP, Ruzicka AE, Assini-Meytin LC, Nair R, et al. Responsible Behavior With Younger Children: Results From a Pilot Randomized Evaluation of a School-Based Child Sexual Abuse Perpetration Prevention Program. Child Maltreat [Internet]. 2024 Feb 1 [cited 2025 Sept 6];29(1):129–41. Available from: https://doi.org/10.1177/10775595221130737

161. Ruzicka AE, Assini-Meytin LC, Schaeffer CM, Bradshaw CP, Letourneau EJ. Responsible Behavior with Younger Children: Examining the Feasibility of a Classroom-Based Program to Prevent Child Sexual Abuse Perpetration by Adolescents. J Child Sex Abuse [Internet]. [cited 2025 Nov 7];30(4). Available from: https://www.prevention.global/resources/responsible-behavior-younger-children-examining-feasibility-classroom-based-program

162. Forum EEC. Cultural Adaptation and Evaluation of the RBYC Program in Germany: Towards Offender-Focused and School-Based Prevention of Child Sexual Abuse [Internet]. Preventing disease and ill health. 2025 [cited 2025 Sept 6]. Available from: https://euspr.hypotheses.org/2100

163. Schatz J, Deesawade R, Mosby W, Kavenagh M. Leaked: Understanding and Addressing Self-Generated Sexual Content Involving Young People in Thailand [Internet]. Evident & HUG Project: Bangkok; 2025 [cited 2025 Nov 4]. Available from: www.itsevident.org/_files/ugd/0bd10b_86d0e7f3921645f7bebc0fa399371860.pdf

164. Dodge A, Lockhart E. "Young People Just Resolve It in Their Own Group": Young People's Perspectives on Responses to Non-Consensual Intimate Image Distribution. Youth Justice J Natl Assoc Youth Justice. 2022 Dec;22(3):304–19.

165. Our story [Internet]. World Childhood Foundation - 25 Years. [cited 2025 Sept 27]. Available from: https://childhood.org/about-childhood/our-story/

166. The HUG Project - Protecting Thai children from sexual abuse and online sex trafficking [Internet]. The HUG Project. [cited 2025 Sept 22]. Available from: https://www.hugproject.org/

167. Evident | Translating evidence into action for social change [Internet]. Evident. [cited 2025 Sept 22]. Available from: https://www.itsevident.org

168. Deterring online child sexual abuse and exploitation: lessons from seven years of campaigning) - Lucy Faithfull Foundation [Internet]. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/deterring-online-child-sexual-abuse-and-exploitation-lessons-from-seven-years-of-campaigning/

169. ReDirection | Protect Children [Internet]. [cited 2025 Sept 22]. Available from: https://www.suojellaanlapsia.fi/en/redirection

170. Help Wanted. Help Wanted Prevention Intervention [Internet]. Help Wanted. [cited 2025 Nov 4]. Available from: https://staging.wp.helpwantedprevention.org/

171. Chatbots and Warning Messages - Innovations in the Fight Against Online Child Sexual Abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/chatbots-and-warning-messages-innovations-in-the-fight-against-online-child-sexual-abuse/

172. Rati. Meri Trustline [Internet]. Rati Foundation. [cited 2025 Nov 4]. Available from: https://ratifoundation.org/meri-trustline/

173. Internet Watch Foundation. IWF 2024: Meri Trustline – Supporting Children Facing Online Harms [Internet]. [cited 2025 Nov 4]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/meri-trustline/

174. UNICEF. Multidisciplinary Models of Care for Child Victims and Survivors of Sexual Abuse and Exploitation in the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/documents/multidisciplinary-models-care-child-victims-and-survivors-sexual-abuse-and-exploitation

175. Prevention Global. Serving Youth Animation, Brieg, Infographic [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.prevention.global/insight/serving-youth-animation-brief-infographic

176. Prevention Global. Serving Youth [Internet]. [cited 2025 Oct 29]. Available from: https://www.prevention.global/serving-youth

177. MyVoiceMySafety-global-poll-of-children.pdf [Internet]. [cited 2025 Sept 22]. Available from: https://www.weprotect.org/wp-content/uploads/MyVoiceMySafety-global-poll-of-children.pdf

178. ECPAT. Guidelines for ethical research on sexual exploitation involving children [Internet]. 2019 [cited 2025 Oct 29]. Available from: https://ecpat.org/guidelines-for-ethical-research/

179. Disrupting Harm: Conversations with Young Survivors about Online Child Sexual Exploitation and Abuse [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/disrupting-harm-conversations-with-young-survivors-about-online-child-sexual-exploitation-and-abuse/

180. Luciana C. Assini-Meytin, McPhail I, Sun Y, Matthews B, Kaufman KL, Letourneau E. Child Sexual Abuse and Boundary Violating Behaviors in Youth Serving Organizations: National Prevalence and Distribution by Organizational Type. Child Maltreat [Internet]. 2024 [cited 2025 Oct 29];20(3):499–511. Available from: https://journals.sagepub.com/doi/10.1177/10775595241290765

181. Alliance WG. Health and wellbeing of frontline responders. 2025 [cited 2025 Sept 27]; Available from: https://www.weprotect.org/wp-content/uploads/Health-and-wellbeing-of-frontline-responders_May-2025.pdf

182. Towards digital safety by design for children | OECD [Internet]. [cited 2025 Sept 22]. Available from: https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html

183. Tech Coalition | Child Safety Best Practices [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/child-safety-best-practices

184. Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment - Livingstone - 2025 - Policy & Internet - Wiley Online Library [Internet]. [cited 2025 Sept 22]. Available from: https://onlinelibrary.wiley.com/doi/10.1002/poi3.70008

185. UNICEF. Assessing child rights impacts in relation to the digital environment | UNICEF Child Rights and Business [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA

186. Digital Futures Commission. Child Rights by Design - 5Rights Foundation & Digital Futures Commission [Internet]. Child Rights By Design | Digital Futures Commission. [cited 2025 Nov 4]. Available from: https://childrightsbydesign.5rightsfoundation.com/

187. Thorn & ATIH. Safety by Design for Generative AI: Preventing Child Sexual Abuse. 2024. Thorn Repository. Available at https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf.

188. Thorn. Safety by Design for responsible AI | Safer by Thorn [Internet]. Purpose-Built Trust and Safety Solutions | Safer by Thorn. 2025 [cited 2025 Nov 4]. Available from: https://safer.io/resources/safety-by-design-a-responsible-ai-framework/

189. Australian Government. Be Secure Quiz | eSafety Commissioner [Internet]. [cited 2025 Nov 4]. Available from: https://www.esafety.gov.au/educators/classroom-resources/be-secure/quiz

190. Human Mobile Devices. HMD Fuse | The phone that grows with your kids [Internet]. HMD - Human Mobile Devices. [cited 2025 Nov 4]. Available from: https://www.hmd.com/en_int/hmd-fuse

191. Apple Support. About Communication Safety on your child's Apple device [Internet]. Apple Support. [cited 2025 Nov 4]. Available from: https://support.apple.com/en-us/105069

192. Snapchat. Parents - Safeguards For Teens [Internet]. [cited 2025 Nov 4]. Available from: https://parents.snapchat.com/safeguards-for-teens

193. Google. Be Internet Awesome [Internet]. Be Internet Awesome. [cited 2025 Nov 4]. Available from: https://beinternetawesome.withgoogle.com/en-us

194. Lego. LEGO® - Code of conduct [Internet]. [cited 2025 Nov 4]. Available from: https://kids.lego.com/en-us/legal/kids-code-of-conduct

195. Instagram. Partner With Instagram to Keep Your Students Safe | About Instagram [Internet]. [cited 2025 Nov 4]. Available from: https://about.instagram.com/community/educators

196. Ngo VM, Gajula R, Thorpe C, Mckeever S. Discovering child sexual abuse material creators' behaviors and preferences on the dark web. Child Abuse Negl. 2024 Jan;147:106558.

197. Haluska R, Badovska M, Pleva M. Concept of Speaker Age Estimation Using Neural Networks to Reduce Child Grooming. Elektron Ir Elektrotechnika. 2024 Aug 26;30(4):61–7.

198. Thorn. Generative AI: Now is the Time for Safety By Design [Internet]. Thorn. 2023 [cited 2025 Nov 4]. Available from: https://www.thorn.org/blog/now-is-the-time-for-safety-by-design/

199. Tech Coalition. Insights to Action: Asia-Pacific Briefing on Combating OCSEA [Internet]. https://technologycoalition.org/. [cited 2025 Nov 4]. Available from: https://technologycoalition.org/news/insights-to-action-tech-coalition-asia-pacific-briefing-on-combating-ocsea/

200. National Center for Missing & Exploited Children. Take It Down [Internet]. Take It Down. [cited 2025 Nov 3]. Available from: https://takeitdown.ncmec.org/

201. Lantern 2024 Transparency Report [Internet]. https://technologycoalition.org/. [cited 2025 Aug 31]. Available from: https://technologycoalition.org/resources/lantern-2024-transparency-report/

202. U.K. Government. Online Safety Act: explainer [Internet]. GOV.UK. [cited 2025 Nov 4]. Available from: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

203. Fiji approves 1st national child safeguarding policy [Internet]. [cited 2025 Sept 22]. Available from: https://english.news.cn/asiapacific/20250822/3042a592ecb344bb8eaa4bd2bf0ebebf/c.html

204. G7 #BeBrave Scorecard Report 2025 [Internet]. Brave Movement. [cited 2025 Sept 27]. Available from: https://www.bravemovement.org/resources/g7-scorecard-2025

205. Global Online Safety Regulators Network. GOSRN Regulatory Index 2024 [Internet]. [cited 2025 Nov 3]. Available from: https://www.esafety.gov.au/sites/default/files/2024-10/GOSRN-Regulatory-Index-2024-final.pdf

206. Tracking the shifts: Age assurance in motion | IAPP [Internet]. [cited 2025 Sept 27]. Available from: https://iapp.org/news/a/tracking-the-shifts-age-assurance-in-motion

207. Taylor J. Not just under-16s: all Australian social media users will need to prove their age – and it could be complicated and time consuming. The Guardian [Internet]. 2025 Sept 1 [cited 2025 Sept 28]; Available from: https://www.theguardian.com/technology/2025/sep/02/under-16s-ban-how-hard-will-it-be-for-australian-social-media-users-to-prove-their-age

208. Department of Infrastructure T. Age assurance consumer research findings [Internet]. Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts; 2025 [cited 2025 Sept 27]. Available from: https://www.infrastructure.gov.au/department/media/publications/age-assurance-consumer-research-findings

209. Faverio MA and M. 81% of U.S. adults – versus 46% of teens – favor parental consent for minors to use social media [Internet]. Pew Research Center. 2023 [cited 2025 Sept 27]. Available from: https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/

210. International A. Social media ban: what is it and what will it mean for young people? [Internet]. Amnesty International Australia. 2024 [cited 2025 Sept 27]. Available from: https://www.amnesty.org.au/social-media-ban-explained/

211. VPNs top App Store charts as UK age verification kicks in [Internet]. 2025 [cited 2025 Sept 27]. Available from: https://www.bbc.com/news/articles/cn72ydj70g5o

212. African Union. African Union Child Online Safety and Empowerment Policy | African Union [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy

213. Commonwealth of Australia. Age Assurance Technology Trial [Internet]. Age Assurance Technology Trial. [cited 2025 Nov 3]. Available from: https://ageassurance.com.au/report/

214. Eltaher F, Gajula R, Miralles-Pechuán L, Thorpe C, McKeever S. The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media. Conf Pap [Internet]. 2025 Jan 1; Available from: https://arrow.tudublin.ie/scschcomcon/442

215. Evershed N, Nicholas J. Social media ban trial data reveals racial bias in age checking software: just how inaccurate is it? The Guardian [Internet]. 2025 Sept 18 [cited 2025 Sept 23]; Available from: https://www.theguardian.com/news/2025/sep/19/how-accurate-are-age-checks-for-australias-under-16s-social-media-ban-what-trial-data-reveals

216. School SL. The "Segregate-and-Suppress" Approach to Regulating Child Safety Online [Internet]. Stanford Law School. 2025 [cited 2025 Sept 28]. Available from: https://law.stanford.edu/publications/the-segregate-and-suppress-approach-to-regulating-child-safety-online/

217. Safe Online. Kenya launches groundbreaking training handbook to combat online child sexual exploitation and abuse [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/kenya-launches-groundbreaking-training-handbook-to-combat-online-child-sexual-exploitation-and-abuse/

218. Thorn. For Victim Identification [Internet]. Thorn. [cited 2025 Nov 3]. Available from: https://www.thorn.org/solutions/victim-identification/

219. Rigr AI. Video Summarisation Tool by Rigr AI [Internet]. Video Summarisation Tool by Rigr AI. [cited 2025 Nov 3]. Available from: https://www.vst.rigr.ai

220. Safe Online Report 2024 – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/safe-online-report-2024/

221. Canadian Framework For Trauma-Informed Response in Policing – Introduction | Barrie Police Service [Internet]. [cited 2025 Sept 27]. Available from: https://www.barriepolice.ca/cftirp-introduction/

222. Landry G. Mobilising the Financial Sector Against the Sexual Exploitation of Children. ECPAT;

223. AFP records spike in financial sextortion reports over the school holidays | Australian Federal Police [Internet]. 2023 [cited 2025 Sept 22]. Available from: https://www.afp.gov.au/news-centre/media-release/afp-records-spike-financial-sextortion-reports-over-school-holidays

224. It's Never Too Early - Early education Project Paradigm collaboration | ACCCE [Internet]. [cited 2025 Sept 22]. Available from: https://www.accce.gov.au/resources/parents-carers/its-never-too-early-early-education-project-paradigm-collaboration

225. Sextortion Campaign [Internet]. Available from: https://www.accce.gov.au/sites/default/files/2022-11/sextortion%20campaign%20video.mp4

226. Prevention Global. Making The Case | Prevention Global [Internet]. [cited 2025 Nov 3]. Available from: https://prevention.global/making-the-case

227. U.S. Government Accountability Office. Science & Tech Spotlight: Deepfakes [Internet]. 2025 [cited 2025 Nov 3]. Available from: https://www.gao.gov/assets/gao-20-379sp.pdf

228. JISC. Digital wellbeing [Internet]. Digital wellbeing. [cited 2025 Nov 3]. Available from: https://digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/

229. Knodel M, Baker F, Kolkman O, Celi S, Grover G. Definition of End-to-end Encryption [Internet]. Internet Engineering Task Force; [cited 2025 Nov 3]. Report No.: draft-knodel-e2ee-definition-04. Available from: https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition-04

230. INHOPE. What is generative AI? [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://inhope.org/EN/articles/what-is-generative-ai

231. Overview of Perceptual Hashing Technology [Internet]. www.ofcom.org.uk. 2022 [cited 2025 Nov 3]. Available from: https://www.ofcom.org.uk/online-safety/safety-technology/overview-of-perceptual-hashing-technology

232. Know2Protect, US Department of Homeland Security. ONLINE ENTICEMENT INFORMATIONAL BULLETIN [Internet]. Available from: https://www.dhs.gov/sites/default/files/2025-01/25_0121_K2P_online-enticement.pdf

233. 'Self-generated' sexual material - WeProtect Global Alliance [Internet]. 2022 [cited 2025 May 1]. Available from: https://www.weprotect.org/issue/self-generated-sexual-material/

weprotect
Global Alliance

CPC
LEARNING
NETWORK

COLUMBIA | MAILMAN SCHOOL OF PUBLIC HEALTH