

Technologies émergentes : risques et opportunités pour la protection des enfants contre l'exploitation sexuelle et les abus sexuels



**Document de réflexion établi
pour le Comité de Lanzarote**

Construire une Europe
pour et avec les enfants



COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Technologies émergentes : risques et opportunités pour la protection des enfants contre l'exploitation sexuelle et les abus sexuels

Document de réflexion établi pour le Comité de Lanzarote

Par Victoria Baines,
professeure et
consultante indépendante

Édition anglaise:

Emerging technologies: threats and opportunities for the protection of children against sexual exploitation and sexual abuse

Les points de vue exprimés dans ce document n'engagent que son auteure et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.

La reproduction d'extraits (jusqu'à 500 mots) est autorisée, sauf à des fins commerciales, tant que l'intégrité du texte est préservée, que l'extrait n'est pas utilisé hors contexte, ne donne pas d'informations incomplètes ou n'induit pas le lecteur en erreur quant à la nature, à la portée et au contenu de ce texte. Le texte source doit toujours être cité comme suit : « © Conseil de l'Europe, année de publication ».

Pour toute autre demande relative à la reproduction ou à la traduction de tout ou partie de ce document, veuillez vous adresser à la Direction de la communication, Conseil de l'Europe (F-67075 Strasbourg Cedex), ou à publishing@coe.int.

Toute autre correspondance relative à ce document doit être adressée au Secrétariat du Comité de Lanzarote, Conseil de l'Europe, F-67075 Strasbourg Cedex, Courriel: lanzarote.committee@coe.int

Conception de la couverture et mise en page : Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale de la DPDP.

© Conseil de l'Europe, octobre 2024
Imprimé dans les ateliers du Conseil de l'Europe

Secrétariat du Comité des Parties à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Comité de Lanzarote)
F-67075 Strasbourg Cedex

lanzarote.committee@coe.int
www.coe.int/lanzarote

Table des matières

CONTEXTE	4
INTELLIGENCE ARTIFICIELLE (IA)	5
IA générative	5
Apprentissage automatique	7
ENVIRONNEMENTS IMMERSIFS – RÉALITÉ VIRTUELLE, RÉALITÉ AUGMENTÉE ET RÉALITÉ ÉTENDUE	8
L'INTERNET DES OBJETS	10
ROBOTIQUE	11
EXPLOITATION ET ABUS SEXUELS CONCERNANT DES ENFANTS DIFFUSÉS EN DIRECT	12
THÉMATIQUES ET QUESTIONS TRANSVERSALES	13

Contexte

■ Le phénomène de l'exploitation et des abus sexuels concernant des enfants est en constante évolution. Qu'ils soient motivés par un intérêt sexuel ou par la perspective d'un avantage financier ou autre, les auteurs de tels actes exploitent pleinement toutes les possibilités qui s'offrent à eux. À l'heure où l'informatique ne cesse de se développer et met de nouveaux outils à disposition des adultes comme des enfants, il importe d'examiner régulièrement les tendances qui émergent, tant du côté des auteurs d'infractions que du côté des victimes, mais aussi d'évaluer le potentiel d'utilisation à mauvais escient des nouvelles technologies afin de s'assurer que les réponses nationales et internationales à l'exploitation et aux abus sexuels concernant des enfants et facilités par la technologie restent adaptées aux besoins.

■ Le présent document invite le Comité de Lanzarote à examiner les répercussions des développements technologiques actuels et futurs sur la nature et l'ampleur de l'exploitation et des abus sexuels concernant des enfants. Les menaces et les possibilités des technologies suivantes sont passées en revue :

- ▶ l'intelligence artificielle (IA générative et apprentissage automatique) ;
- ▶ la réalité étendue, comprenant la réalité virtuelle, la réalité augmentée et d'autres environnements numériques immersifs ;
- ▶ les innovations robotiques ;
- ▶ l'internet des objets ;
- ▶ la génération et la diffusion de vidéos en direct.

Intelligence artificielle (IA)

IA générative

■ L'« intelligence artificielle » (IA) est le terme générique employé pour décrire deux types d'outils numériques avancés. Le premier est l'IA générative, dont l'application la plus connue est ChatGPT et qui consiste en de grands modèles de langage (LLM) entraînés pour produire des textes et des images en imitant des modèles dans des ensembles de données préexistants. Si les textes ainsi créés semblent naturels et plausibles, ils ne sont pas nécessairement ni totalement conformes aux faits. Plus les données d'entraînement sont riches et détaillées, plus le texte généré est complet et convaincant, qu'il s'agisse d'une réponse à une demande d'informations factuelles ou d'une tâche de production de contenu d'ordre général dans un format standard, comme du matériel de marketing ou un courrier officiel. L'IA générative peut aussi servir à écrire et à vérifier les codes de programmes informatiques. La fonctionnalité de génération de texte sert de plus en plus à alimenter les conversations que nous avons avec des robots, par exemple, dans les chats de service client non humain sur les sites internet et dans les médias sociaux. Nous avons vu apparaître récemment des applications servant à créer un compagnon ou partenaire d'IA avec lequel l'utilisateur peut interagir. Certaines d'entre elles sont des extensions officielles de services de médias sociaux, à l'image de « My IA » de Snapchat¹. D'autres sont des applications autonomes qui permettent, par exemple, de créer une petite amie ou un petit ami virtuel personnalisable ou encore de reproduire en version numérique un être cher décédé pour pouvoir continuer à discuter et à interagir avec lui en ligne.

■ Si ces applications peuvent effectivement contribuer à apaiser la solitude et apporter du réconfort à ceux qui en éprouvent le besoin, en revanche, il y a un risque qu'elles soient détournées de leur but initial, notamment pour nuire aux enfants. Les applications d'amis virtuels peuvent amener des enfants et des jeunes à prendre part à des conversations sur des sujets liés à la sexualité qui ne sont pas adaptées à leur âge et qui constitueraient une infraction criminelle dans certaines juridictions si elles étaient commises par un être humain adulte. Les prédateurs peuvent exploiter les failles de cybersécurité d'applications ou d'ordinateurs de victimes potentielles et pirater ces dispositifs pour se faire passer pour un ami ou un proche. Il n'est pas indispensable d'avoir des compétences techniques pointues pour cela puisqu'il suffit, par exemple, de persuader l'enfant de communiquer le mot de passe de son compte. De manière plus générale, les robots pourraient servir à automatiser les approches de sollicitation à des fins sexuelles et ainsi permettre à un seul auteur d'infractions d'entrer en contact avec un grand nombre d'enfants.

■ En matière d'images et de vidéos, l'IA générative peut être utilisée pour produire du contenu de synthèse entièrement nouveau ou pour modifier du matériel existant. Des outils accessibles au public, tels que DALL-E et Midtravel, offrent ces deux possibilités aux utilisateurs, tout en étant dotés de dispositifs de protection qui empêchent de générer des images à caractère sexuel. En revanche, certaines applications de « face swapping », qui permettent de remplacer le visage ou le corps d'une personne par un autre sur des photos ou dans des vidéos, sont exploitées par des entreprises moins fiables qui laissent la possibilité aux utilisateurs de télécharger des photos ou vidéos de personnes réelles, puis de les modifier pour produire du contenu à caractère sexuel. Des cas de jeunes faisant circuler du matériel produit à partir d'applications de « déshabillage » à l'insu de camarades ont ainsi été signalés². Dans le domaine connexe de la cybercriminalité, le clonage d'enregistrements audio sert déjà à piéger des personnes à des fins d'escroquerie.

1. <https://help.snapchat.com/hc/fr-fr/articles/13266788358932-Qu'est-ce-que-My-AI-sur-Snapchat-et-comment-puis-je-l-utiliser>
2. <https://www.bbc.co.uk/news/world-europe-66877718>; <https://www.bbc.co.uk/news/technology-67521226>

■ De plus en plus d'images et de vidéos réalistes truquées (deepfakes) d'enfants réels, qui constituent du matériel d'abus sexuels sur des enfants tel que visé par l'article 20 de la Convention de Lanzarote, circulent sur le web clandestin comme sur le web ouvert³. Cette situation soulève plusieurs questions, parmi lesquelles la possibilité d'utiliser des images et des vidéos truquées comme moyen de pression pour amener une victime à produire elle-même de « vraies » images et vidéos à caractère sexuel, potentiellement visées par les articles 21 et 23 de la Convention de Lanzarote. Les réponses de la justice et de la législation pénales peuvent être remises en question dès lors qu'il n'y a aucune preuve tangible d'infraction sexuelle commise contre l'enfant, alors même que l'impact émotionnel sur les victimes est bien réel⁴.

Pistes de réflexion

- ▶ Comment devrait-on évaluer les répercussions sur les victimes : i) de l'exploitation et des abus sexuels hors ligne ; ii) des matériels d'abus sexuels sur des enfants obtenus par sollicitation ; iii) des images et vidéos à caractère sexuel autogénérées par des enfants qui sont utilisées à mauvais escient ; et iv) des matériels d'abus sexuels sur des enfants générés par l'IA et ne représentant pas d'enfants réels ?
- ▶ La production et la diffusion d'images et de vidéos à caractère sexuel autogénérées par des enfants et qui représentent un enfant réel dans un scénario sexuel fictif devraient-elles être considérées comme une infraction moins grave que l'utilisation de matériel d'abus sexuels sur des enfants constituant une infraction sexuelle, et sur quel fondement ?
- ▶ Quelle réponse réglementaire (et sociétale) est adéquate en cas de production et de diffusion par d'autres enfants ou jeunes de deepfakes représentant des abus sexuels commis sur des enfants ?
- ▶ Des solutions techniques peuvent-elles être exigées pour empêcher le trucage d'images et de vidéos impliquant des enfants ?

■ Ces questions s'étendent également à la production et à la diffusion de matériels d'abus sexuels sur enfants entièrement réalisés au moyen de technologies de synthèse et qui ne présentent pas de ressemblance avec un enfant existant. Cet aspect relève en particulier de l'article 20 de la Convention de Lanzarote selon lequel la production, l'offre ou la mise à disposition, la diffusion ou la transmission, le fait de se procurer, la possession et l'accès en connaissance de cause à du matériel d'abus sexuels sur des enfants constituent des infractions. L'article 20, paragraphe 3, dispose que les États peuvent se réserver le droit d'exclure de la portée de ces infractions la production et la possession de matériel d'abus sexuels « constitué exclusivement de représentations simulées ou d'images réalistes d'un enfant qui n'existe pas ». Il est en effet possible, depuis plusieurs années, de créer des images de personnes qui ne sont pas réelles⁵. Par le passé, les mesures législatives de protection de l'enfance accordaient la priorité à la répression concernant les matériels d'abus sexuels sur des enfants au motif qu'ils représentent la commission d'infractions sexuelles subies par des enfants réels. Lorsqu'il n'est pas question d'enfants réels, peut-on invoquer le même fondement ou faut-il qu'il y ait un autre fondement, tel que le caractère d'obscénité ? Faut-il adopter une approche différente axée sur le risque que présentent les personnes qui s'intéressent aux matériels d'abus sexuels générés par l'IA ou sur le potentiel de corruption d'enfants ? On pourrait imaginer, par exemple, que les personnes qui cherchent à solliciter des enfants à des fins sexuelles partagent du matériel d'abus sexuels produit par l'IA avec des victimes potentielles afin de banaliser l'activité sexuelle entre adultes et enfants.

Pistes de réflexion

- ▶ S'il n'y a pas d'enfants « réels » représentés dans les matériels d'abus sexuels, quelles sont les réponses adéquates en matière de réglementation et de sanctions ?
- ▶ Les auteurs d'infractions de ce type présentent-ils moins de risques pour les enfants que ceux qui possèdent du matériel d'abus sexuels commis sur des enfants « réels » ?
- ▶ Peut-on exiger des solutions techniques qui empêchent la création d'images, de vidéos ou de chatbots d'enfants ?

3. <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/>

4. <https://www.bbc.co.uk/news/articles/cpdlpj9zn9go>

5. <https://thispersondoesnotexist.com/>

Apprentissage automatique

■ Si l'on parle beaucoup plus d'IA générative que d'apprentissage automatique, l'impact de ce deuxième champ de l'IA sur la société est tout aussi considérable. L'apprentissage automatique désigne le développement d'algorithmes à partir de données, qui donnent lieu à des modèles et à la résolution de tâches sans instruction explicite. L'analyse prédictive, la vision par ordinateur, le traitement du langage naturel et la reconnaissance vocale sont autant d'exemples d'application de cette technologie.

■ L'apprentissage automatique est largement utilisé pour lutter contre l'exploitation et les abus sexuels concernant des enfants, en particulier sur les plateformes en ligne. Des entreprises investissent dans le développement d'outils qui signalent les comportements suspects ou non authentiques en se fondant sur l'analyse de très grands ensembles de métadonnées de comptes, ainsi que dans l'examen et la classification de contenu en vue d'identifier le matériel illégal à signaler. À force d'entraînement et d'apprentissage, la précision et la capacité de détection des outils s'améliorent sans cesse, ce qui se traduit par une augmentation du nombre de comptes dont l'activité suspecte est détectée et du volume de contenu d'exploitation et d'abus sexuels concernant des enfants signalé aux forces de l'ordre. De la même manière, ce procédé peut aider les plateformes à identifier des indicateurs d'exploitation et d'abus sexuels qui passaient jusque-là inaperçus et dont le signalement aux autorités n'a pas de fondement juridique évident.

■ Cela étant, l'examen et la classification du contenu dépendent de la capacité des plateformes à afficher du contenu non chiffré, ce qui signifie que le chiffrement de bout en bout devient problématique lorsqu'il s'agit d'examiner du contenu. Les solutions qui proposent l'analyse de matériel illégal sur l'appareil d'utilisateurs (analyse côté client) ont été bien accueillies par les spécialistes de la protection de l'enfance, mais rejetées par les défenseurs du respect de la vie privée, qui craignent que la technologie ne serve à rechercher du contenu autre que celui lié à l'exploitation et aux abus sexuels concernant des enfants.

■ À l'inverse, l'apprentissage automatique peut aider les auteurs d'infractions. L'IA sert de plus en plus à automatiser la collecte d'informations en libre accès⁶. Les outils permettant d'explorer et d'analyser de grands ensembles de données peuvent être utilisés à des fins légitimes, mais aussi par des criminels pour atteindre leurs cibles. Puisque l'on sait déjà que les auteurs d'infractions telles que la sollicitation et l'extorsion à des fins sexuelles recherchent des victimes potentielles et interagissent avec elles sur de multiples plateformes, on peut aisément imaginer qu'elles cherchent à automatiser ce processus pour le rendre plus efficace et adapté à la recherche d'un plus grand nombre de victimes.

Pistes de réflexion

- ▶ À mesure que les techniques de signalement des activités suspectes s'améliorent, quels aspects sont à prendre en compte concernant la charge de travail des forces de l'ordre dans le monde entier ? Existe-t-il un fondement juridique suffisant pour que les plateformes partagent des données sur l'exploitation et les abus sexuels concernant des enfants qui n'atteignent pas les niveaux de preuve en vigueur ?
- ▶ Alors que le chiffrement de bout en bout devient la norme pour les services de messagerie, comment les plateformes et les autorités parviendront-elles à identifier les contenus et activités illicites et à en fournir la preuve ?
- ▶ Une solution technique peut-elle être imposée pour empêcher que les données concernant des enfants ne soient exploitées par les auteurs d'infractions relevant de l'exploitation et des abus sexuels ?

6. <https://www.oii.ox.ac.uk/news-events/open-source-intelligence-osint-and-ai-the-informational-pivot-of-intelligence-analysis/>

Environnements immersifs – réalité virtuelle, réalité augmentée et réalité étendue

■ La frontière entre notre monde physique et notre monde numérique est aujourd’hui très floue. La réalité augmentée améliore nos expériences hors ligne en y superposant des données, que nous utilisons une application de cartographie ou que nous jouons à un jeu sur application mobile tel que Pokémon Go. Dans la réalité virtuelle, le matériel, notamment le casque et les dispositifs de commande avec rétroaction haptique (ressenti tactile), nous plonge dans une expérience à 360° dans laquelle nous nous sentons émotionnellement et, de plus en plus, physiquement présents. L’utilisation de périphériques dans l’informatique sociale n’est pas nouvelle en soi, puisqu’on utilise des joysticks, des volants et même des armes connectées depuis des dizaines d’années. De même, les joueurs en ligne ont l’impression d’être « vraiment présents » dans les mondes virtuels depuis tout aussi longtemps. Les améliorations récentes de la vitesse et de la fiabilité d’internet, associées à des investissements considérables de la part des sociétés de jeux, ont abouti au développement de mondes virtuels de plus en plus riches et attrayants, dont certains permettent l’intégration d’appels vidéo et de médias sociaux « réels » dans des environnements informatisés.

■ Compte tenu du marché bien établi des matériels d’abus sexuels sur des enfants, l’existence d’une demande d’expériences sexuelles immersives impliquant des enfants, qui peut soulever des questions au titre de l’article 20 de la Convention de Lanzarote, n’aura rien de surprenant. Sur des plateformes telles que Virt-A-Mate, qui permettent à l’utilisateur de créer son partenaire sexuel idéal, les forces de l’ordre ont signalé que des avatars d’enfants étaient créés à cette fin. De même, selon les données de la police, des matériels d’abus sexuels sur des enfants ont déjà été trouvés dans des casques de réalité virtuelle⁷.

■ Lors d’une récente table ronde organisée par WeProtect Global Alliance, il a été noté que les approches de sollicitation d’enfants à des fins sexuelles dans des environnements immersifs pouvaient également être plus convaincantes, donc plus efficaces⁸. Comme constaté dans d’autres environnements de jeux en ligne, les enfants sont très attirés par les récompenses, les prix et d’autres articles virtuels, qui risquent donc d’être instrumentalisés pour les inciter ou les contraindre à produire eux-mêmes des images et vidéos à caractère sexuel ou à pratiquer une activité sexuelle, ce qui peut constituer une infraction au titre des articles 20 à 23 de la Convention de Lanzarote.

■ Le caractère immersif des mondes virtuels peut s’avérer problématique pour les acteurs de la justice pénale lors de la collecte et de la présentation de preuves. Les services répressifs qui sont habitués à demander des fichiers contenant des conversations textuelles, des images statiques et des vidéos enregistrées, souvent au-delà des frontières nationales, peuvent estimer que ces éléments ne suffisent pas à prouver que la victime présumée a effectivement vécu une mauvaise expérience immersive en ligne. La complexité et l’ampleur des environnements immersifs ne permettent pas aux plateformes d’enregistrer l’intégralité des expériences des utilisateurs de sorte qu’elles puissent être présentées devant un tribunal. Pour cette raison, certains fournisseurs de plateformes ont recommandé aux utilisateurs d’enregistrer toutes leurs activités et expériences au fur et à mesure, au cas où il serait nécessaire de fournir aux autorités les preuves d’un crime présumé.

■ De toute évidence, l’exploitation et les abus sexuels concernant des enfants en milieu immersif ne relèvent plus d’une hypothétique menace⁹. En 2018, dans une affaire qui a retenu l’attention dans le monde entier, une fillette américaine de 7 ans a vu son avatar du jeu Roblox subir un « viol collectif » commis par deux avatars masculins adultes. Indépendamment des considérations juridiques, la description faite par la mère des

7. <https://www.bbc.co.uk/news/uk-64734308>

8. <https://www.weprotect.org/library/beyond-the-headset-extended-reality/>

9. <https://www.bbc.co.uk/news/technology-44697788>

répercussions de cette agression sur son enfant a clairement montré qu'elle n'était pas simplement vécue comme un « crime virtuel », mais bien comme un événement réellement traumatisant sur le plan émotionnel. De même, il y a quelques mois, la police britannique a annoncé qu'elle enquêtait sur des abus sexuels commis dans la réalité virtuelle sur une jeune fille de moins de 16 ans¹⁰. Alors que le sentiment de présence émotionnelle et physique est de plus en plus fort dans les environnements immersifs, il convient de se demander si la distinction pratique faite actuellement dans la législation de nombreux pays entre les crimes d'exploitation et d'abus sexuels concernant des enfants commis en ligne et ceux commis hors ligne tient dûment compte des répercussions pour les victimes de ce type d'expériences dans des environnements immersifs et couvre suffisamment des infractions vécues comme étant réelles, même lorsqu'il n'y a pas de préjudice physique.

Pistes de réflexion

- ▶ Les procédures pénales actuelles permettent-elles la collecte de preuves électroniques à partir de mondes virtuels immersifs, et quelles sont les considérations pratiques à cet égard ?
- ▶ Peut-on imposer une solution technique empêchant les utilisateurs adultes de créer des avatars d'enfants ? Comment pourrait-on faire appliquer une telle règle ?
- ▶ L'exposition d'enfants à du contenu immersif à caractère sexuel devrait-elle constituer une infraction plus grave que le fait d'amener des enfants à regarder des vidéos et des images statiques ?
- ▶ Peut-on imposer une solution technique qui empêcherait les enfants d'être en contact avec du contenu ou des activités à caractère sexuel ? Comment pourrait-on faire appliquer une telle règle ?

10. <https://news.sky.com/story/police-investigate-sexual-abuse-of-young-girls-avatar-in-the-metaverse-prompting-nspcc-warning-13041003>

L'internet des objets

■ La notion d'abus sexuels dans les environnements numériques immersifs est liée au développement continu de technologies qui connectent des objets à internet et les uns aux autres, ce que l'on désigne communément par l'« internet des objets ».

■ Outre les appareils domestiques intelligents et certains équipements essentiels, la connectivité est de plus en plus présente dans des articles tels que les sex-toys, dont le marché de détail s'est considérablement développé au plus fort de la pandémie de covid. On trouve maintenant en vente libre des jouets pour adultes qui peuvent être contrôlés à distance par un partenaire à l'aide d'une application et qui peuvent être connectés à des plateformes de divertissement pour adultes telles qu'OnlyFans. Il est désormais possible d'intégrer ces appareils dans des expériences sexuelles de réalité virtuelle. La pornographie est déjà bien plus que de la vidéo : elle aussi devient de plus en plus une affaire d'expérience et de participation directe.

■ On peut donc tout à fait s'attendre à ce que des enfants soient exposés à de la pornographie associée à des appareils connectés (article 22 de la Convention de Lanzarote). Compte tenu des nouveaux indicateurs cités précédemment d'exploitation sexuelle d'enfants dans la réalité virtuelle, les autorités devraient également se préparer à des cas d'abus sexuels sur des enfants facilités par des sex-toys connectés, notamment à des cas d'enfants soumis à une sensation physique déclenchée à distance par un adulte ou qui sont incités à provoquer cette sensation sur eux-mêmes ou sur d'autres enfants. Il existe certainement des arguments solides pour qualifier ces agissements d'abus sexuels commis sur des enfants (article 18 de la Convention de Lanzarote) plutôt que d'infractions impliquant du matériel d'abus sexuels sur des enfants (article 20 de la Convention de Lanzarote), du spectacle pornographique (article 21 de la Convention de Lanzarote) ou de la corruption d'enfants (article 22 de la Convention de Lanzarote), qui donnent lieu à des peines moins sévères dans certaines juridictions.

■ De manière plus générale, des études ont montré qu'une cybersécurité défaillante des appareils connectés tels que des jouets pour enfants ou des babyphones permettrait à des adultes inconnus d'avoir accès aux enfants sur leur lieu de vie. En l'absence de mesures de sécurité efficaces, les caméras, les haut-parleurs et les microphones intégrés dans ces appareils peuvent être activés à distance pour discuter avec des enfants et capturer des images d'eux¹¹. Ces dernières années, beaucoup de pays (mais pas tous) ont instauré une législation pour améliorer la sécurité de l'internet des objets en rendant obligatoires l'utilisation de mots de passe uniques, la notification des failles de sécurité et les mises à jour de sécurité pour les appareils connectés aux consommateurs. Ces solutions réglementaires n'excluent pas cependant la possibilité d'un accès à distance aux enfants par ingénierie sociale, par exemple, en persuadant l'enfant ou une personne s'occupant de lui de divulguer son mot de passe, ce qu'il convient de traiter par la sensibilisation et l'éducation à ce sujet.

Pistes de réflexion

- ▶ Existe-t-il une couverture législative suffisante pour garantir la sécurité des appareils domestiques et jouets pour enfants connectés ? Est-ce que cela permet de décourager les pratiques laxistes et de prévenir les abus, y compris l'exploitation et les abus sexuels, de manière efficace ?
- ▶ Le public est-il suffisamment sensibilisé à la nécessité de sécuriser les appareils connectés par une bonne hygiène informatique ? Comment pourrait-on améliorer cela ?
- ▶ Peut-on imposer une solution technique pour empêcher les enfants d'utiliser des sex-toys connectés pour adultes ? Et comment pourrait-on faire respecter une telle mesure ?

11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407264;making-childrens-toys-swear/

<https://www.pentestpartners.com/security-blog/>

Robotique

■ Plusieurs entreprises ont développé des robots compagnons à des fins d'activité sexuelle hors ligne, dont les propriétaires peuvent spécifier l'apparence et les mensurations et personnaliser les expressions, la voix, les réactions verbales et physiques et le caractère. Les robots sexuels les plus sophistiqués combinent le mouvement animatronique avec l'apprentissage automatique et l'IA générative. Des efforts, des ressources et un temps considérables sont consacrés à les rendre suffisamment réalistes et conformes sur le plan anatomique pour que les gens soient prêts à y mettre le prix, qui peut atteindre des milliers de dollars. Pour l'instant du moins, ces robots ne sont pas à la portée de tous et restent réservés aux plus riches. Par ailleurs, les principales entreprises qui participent à leur développement interdisent les commandes de robots à l'effigie d'enfants. Les progrès réalisés en robotique doivent être pris en compte pour ce qui est d'imposer des dispositions réglementaires concernant les robots à l'effigie d'enfants, de la même manière que les poupées sexuelles représentant des enfants font l'objet d'une réglementation¹².

Pistes de réflexion

- ▶ Les images ou vidéos d'un adulte qui se livre à des activités sexuelles avec une poupée à l'effigie d'un enfant relèvent-elles du matériel d'abus sexuel commis sur des enfants ?
- ▶ La fabrication, l'importation et l'exportation de poupées sexuelles à l'effigie d'enfants devraient-elles être interdites ? Comment pourrait-on faire respecter une telle interdiction ?

12. <https://www.bbc.co.uk/news/uk-41203239>; <https://journals.sagepub.com/doi/10.1177/1023263X231176908>; <https://www.cps.gov.uk/legal-guidance/sex-dolls-childlike>

Exploitation et abus sexuels concernant des enfants diffusés en direct

■ Depuis quelques années, on voit avec quelle rapidité les infractions liées à l'exploitation et aux abus sexuels concernant des enfants sont désormais commises. De la production « en studio » de matériel d'abus sexuels sur des enfants à la sollicitation d'images et de vidéos à caractère sexuel autogénérées par des enfants, on est passé à la diffusion de vidéos en direct à l'aide de plateformes et de technologies audiovisuelles accessibles à un large public.

■ Cela fait maintenant plusieurs années que des matériels d'exploitation sexuelle d'enfants à des fins commerciales sont diffusés en direct. Avec l'amélioration de la qualité et de la vitesse de connexion, les clients spectateurs peuvent désormais passer commande d'un abus commis à distance dans un autre pays, avec des instructions et des demandes spécifiques. Des États parties ont donc commencé à poursuivre des personnes pour avoir participé à une infraction de ce type, pour l'avoir commise ou pour avoir incité à commettre l'infraction. En 2013, un homme de 52 ans a été condamné en Suède à huit ans d'emprisonnement pour onze cas d'incitation flagrante au viol d'un enfant aux Philippines. Au Royaume-Uni, l'application de la compétence extraterritoriale à la législation sur l'exploitation et les abus sexuels concernant des enfants a permis aux autorités de poursuivre en justice des délinquants pour incitation à distance à l'abus sexuel d'enfants aux Philippines.

■ Le Comité a bien conscience que l'intégration de caméras dans les appareils mobiles augmente le risque que des enfants et des jeunes soient sollicités, exploités ou contraints de produire et de partager des images et vidéos à caractère sexuel, dont certaines se retrouvent sur des plateformes pour adultes. Cela soulève la question de savoir si les fournisseurs prennent suffisamment de mesures pour bannir de leurs services les images et les vidéos d'enfants à caractère sexuel. Des initiatives de partenariats innovants ont été lancées, à l'image de StopNCII.org, permettant à des personnes (y compris des enfants) qui ont partagé des images intimes d'elles-mêmes de communiquer des empreintes numériques à de grandes plateformes déployées à l'échelle mondiale pour qu'elles empêchent le téléchargement de ces images par d'autres personnes¹³.

■ Lorsque des images et des vidéos à caractère sexuel autogénérées par des enfants sont publiées ou communiquées d'une autre manière sans leur consentement, qu'elles soient obtenues par d'autres enfants ou par la sollicitation ou sous la contrainte d'un adulte, une course contre la montre s'engage alors pour veiller à ce que le matériel soit retiré de la circulation le plus rapidement possible et ainsi éviter la revictimisation. Lorsqu'il est question d'extorsion sexuelle et de vidéos en direct, la réponse à l'exploitation et aux abus sexuels d'enfants nécessite de plus en plus une intervention d'urgence pour protéger l'enfant en situation de crise. Or, bien souvent, les structures de justice pénale n'ont pas cette souplesse d'action, en particulier lorsque la divulgation de données à l'échelle internationale s'avère nécessaire. Les nouvelles technologies peuvent néanmoins apporter des solutions pour accélérer le retrait des matériels en cause et empêcher leur partage ou leur publication répétée dès lors qu'ils ont été signalés par la victime.

Pistes de réflexion

- ▶ La couverture réglementaire est-elle suffisante pour lutter contre la sollicitation, l'exploitation ou la contrainte d'enfants à des fins de production d'images et de vidéos à caractère sexuel autogénérées en direct ?
- ▶ Une solution technique permettrait-elle de renforcer les efforts de prévention à cet égard ?
- ▶ Les pouvoirs procéduraux sont-ils suffisamment souples pour permettre aux services répressifs et à la justice pénale de réagir immédiatement aux abus et à la coercition qui se déroulent en direct ?

13. <https://stopncii.org/partners/industry-partners/>

Thématiques et questions transversales

Plusieurs thématiques et questions récurrentes se dégagent de l'analyse qui précède. Tout d'abord, la question se pose de savoir qui devrait être responsable de la prévention et de la lutte contre l'exploitation et les abus sexuels facilités par la technologie. Si la réponse de la justice pénale reste de toute évidence nécessaire, les services en ligne ont aussi un rôle à jouer puisqu'ils ont un accès exclusif à des informations privilégiées sur l'utilisation abusive de leurs plateformes. De plus, comme indiqué précédemment, leur coopération est souvent essentielle pour dissiper le sentiment de crise d'enfants victimes d'extorsion sexuelle et lorsque des images et vidéos qu'ils ont eux-mêmes générées sont publiées sans leur consentement. **La responsabilité des personnes morales (Article 26 de la Convention de Lanzarote)** fait naturellement figure de priorité parmi les efforts déployés en matière législative pour prévenir les préjudices subis par les enfants en ligne. À cet égard, la loi britannique sur la sécurité en ligne et la loi européenne sur les services numériques figurent parmi les instruments récents qui visent à établir un référentiel de conformité, à parvenir à une plus grande transparence et à garantir que les conditions d'utilisation des plateformes sont effectivement appliquées.

En l'absence d'interdiction à l'échelle mondiale des applications de déshabillage et des outils de création de deepfakes, **l'éducation des enfants (article 6 de la Convention de Lanzarote)** à une utilisation appropriée de la technologie, au respect du contenu numérique d'autrui et au principe de consentement s'impose de toute urgence. Dans son Avis de 2019, le Comité de Lanzarote a examiné la question du partage non consenti, par d'autres enfants, d'images et de vidéos à caractère sexuel autogénérées par des enfants, qui impose de trouver rapidement des solutions compte tenu de la capacité des jeunes à créer des images et des vidéos sexualisées de leurs pairs¹⁴.

De même, au vu des répercussions émotionnelles et physiques considérables des technologies immersives à des fins d'exploitation et d'abus sexuels concernant des enfants, il est essentiel de fournir aux victimes une assistance psychosociale et un accompagnement thérapeutique continu, comme indiqué dans la Convention de Lanzarote, notamment dans les articles relatifs à **l'assistance aux victimes (article 14), aux programmes ou mesures d'intervention préventive (article 7) et aux programmes ou mesures d'intervention (Chapitre V de la Convention de Lanzarote) destinés aux auteurs d'infractions**. Les preuves de plus en plus nombreuses des répercussions émotionnelles et physiques de l'exploitation et des abus sexuels concernant des enfants en ligne peuvent également nous amener à revoir les sanctions imposées en cas d'infractions commises hors ligne et sans contact physique entre l'auteur et la victime et à déterminer si les distinctions juridiques et conceptuelles entre les infractions commises en ligne et celles commises hors ligne sont toujours adéquates. Ce point peut être particulièrement pertinent lorsque la fourniture d'un soutien aux victimes ou l'intervention concernant les auteurs dépendent de la gravité de l'infraction telle qu'établie dans le droit interne.

Le développement des TIC offre la possibilité aux auteurs d'infractions relevant de l'exploitation et des abus sexuels concernant des enfants de profiter d'espaces perçus comme étant « sûrs », dans lesquels ils peuvent se retrouver, partager leur savoir et commettre des infractions. Comme l'illustre le débat actuel sur le chiffrement de bout en bout, il faut envisager d'autres approches de détection, d'enquête et de collecte de preuves. Il s'agit notamment de veiller à ce que les services répressifs disposent de l'autorité et des capacités nécessaires pour mener des **enquêtes discrètes (article 30 de la Convention de Lanzarote)** sur toutes les infractions d'exploitation et d'abus sexuels concernant des enfants et à ce que **les unités spécialisées dans ce type d'enquêtes** disposent de ressources adéquates **(article 34 de la Convention de Lanzarote)**.

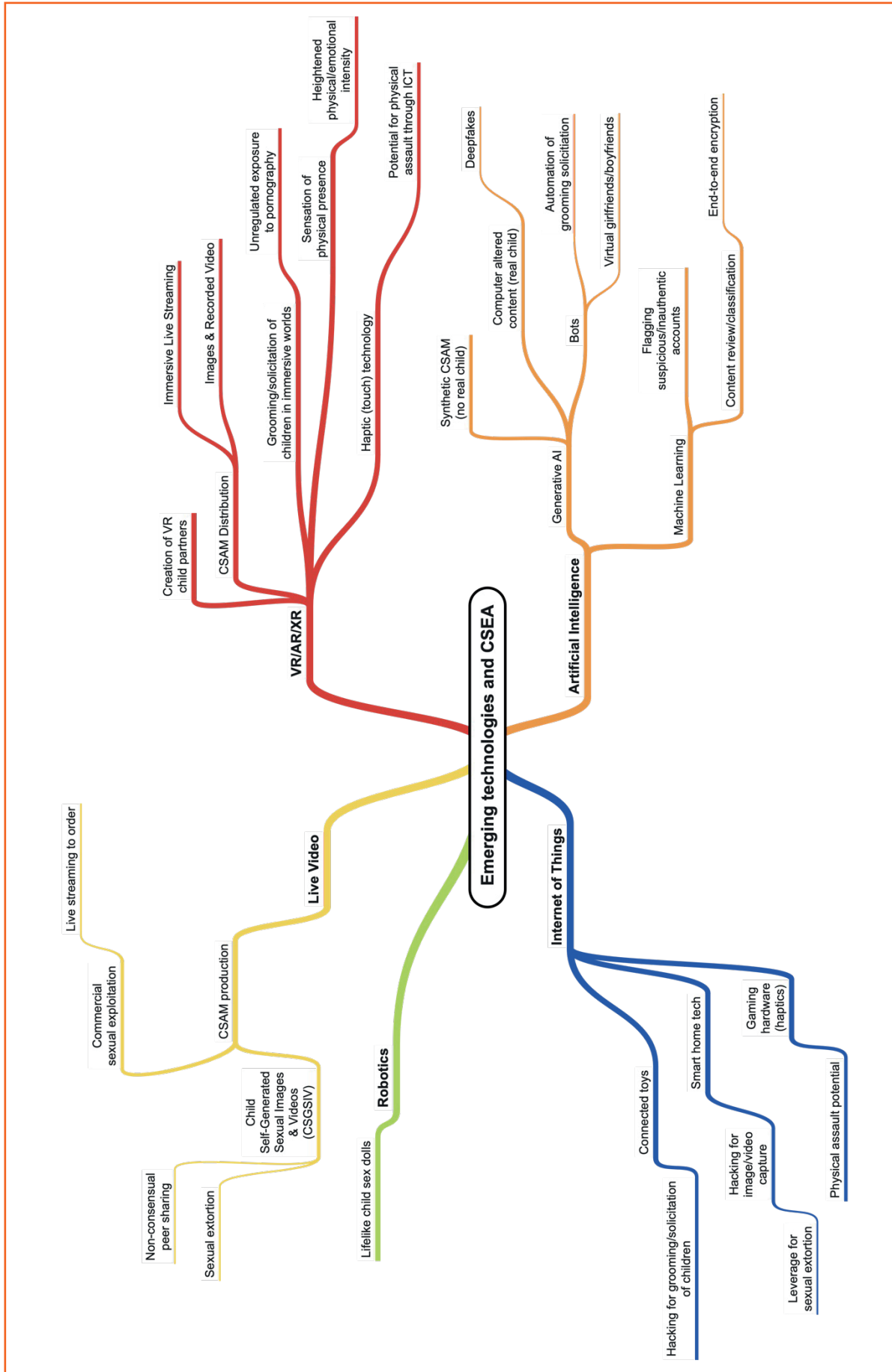
Nous pourrions également examiner comment ces technologies peuvent être mises à profit pour prévenir et combattre l'exploitation et les abus sexuels concernant des enfants plutôt que de simplement les laisser contribuer à leur prolifération. Des lignes d'assistance téléphonique pour enfants et des centres pour un internet plus sûr utilisent déjà des chatbots alimentés par l'IA pour conseiller directement les enfants et les jeunes. Diverses initiatives s'appuient également sur les chatbots pour intervenir auprès des auteurs d'infractions et des personnes qui risquent d'en commettre, par exemple, lors de la recherche de matériels d'abus sexuels commis sur des enfants diffusés sur des sites internet pour adultes¹⁵. Dans d'autres domaines stratégiques, la réalité virtuelle est utilisée pour faire vivre une expérience empathique, par exemple, avec des personnes atteintes de démence ou de jeunes réfugiés¹⁶. La grande question qui se pose est donc la suivante : comment les acteurs de la lutte contre l'exploitation et les abus sexuels concernant des enfants pourraient-ils mettre les développements technologiques au service de leur cause et de celle des enfants ?

14. <https://rm.coe.int/avis-du-comite-de-lanzarote-sur-les-images-et-ou-videos-d-enfants-sexu/168094e72f>

15. <https://www.iwf.org.uk/news-media/news/pioneering-chatbot-reduces-searches-for-illegal-sexual-images-of-children/>

16. <https://www.awalkthroughdementia.org/> ; <https://www.with.in/watch/clouds-over-sidra/>

Carte mentale – Exploitation et abus sexuels d'enfants facilités par les technologies émergentes



www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits humains du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits humains, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE